TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

RIIKKA PEURA

MARITIME CYBERSECURITY AND IMPROVEMENT OF PROJECT EXECUTION PROCESS

Master of Science Thesis

Examiner: prof. Jose Luis Martinez Lastra
Examiner and topic approved by the Faculty Council of the Faculty of Engineering Sciences on 31 May 2017

ABSTRACT

RIIKKA PEURA: Maritime Cybersecurity and Improvement of Project Execution Process
Tampere University of Technology
Master of Science Thesis, 73 pages, 2 Appendix pages
November 2017
Master's Degree Programme in Automation Technology
Major: Factory Automation
Examiner: Professor Jose Luis Martinez Lastra

Keywords: cybersecurity, maritime industry, project execution, process improvement

The increasing complexity, digitalization, integration and automation of the maritime systems set new cybersecurity requirements for the whole maritime sector. This thesis investigates the newest cybersecurity publications guiding the industry including releases of standardization and maritime organizations and classification societies. The goal of the research is to improve and unify the cybersecurity project execution process of a global company delivering electrification and automation solutions for the industry.

The research consists of two parts: a literature and industrial practices review and a practical part aiming at the identification of key areas of focus for the company from which to begin the unification of their cybersecurity project execution process. The literature review demonstrates the industry's ruling approach on cybersecurity: holistic cyber risk management through each organization level. The review was used as a theoretical framework for the empirical part based on workshops with cybersecurity responsible persons from different local business units of the company.

This thesis provides a methodology for global process unification, a list of identified improvement areas of the current cybersecurity project execution process of the company and suggestions for improvement. All the list items will be improved, but four key areas of focus are prioritized: inadequate global infrastructure and standardized cybersecurity project execution process, training, conflicts between global and local cybersecurity guidelines and technical solutions and procedures for cybersecurity execution. As a result of this thesis, the company began enhancing of a global cybersecurity information sharing platform, complementing training to become globally valid, clarifying conflicts between global and local guidelines and developing a new cybersecurity execution service solution.

Overall, this thesis provides the reader with an overview of the current cybersecurity situation of the maritime industry and helps the preparation for future requirements. This thesis also presents practical suggestions for the cybersecurity related issues the project organization of the company is facing. The development processes started during this thesis will be continued under the group level globalization of security policies.

TIIVISTELMÄ

RIIKKA PEURA: Meriteollisuuden kyberturvallisuus ja projektiprosessin parannus
Tampereen teknillinen yliopisto
Diplomityö, 73 sivua, 2 liitesivua
Marraskuu 2017
Automaatiotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Factory Automation
Tarkastaja: professori Jose Luis Martinez Lastra

Avainsanat: kyberturvallisuus, meriteollisuus, projektointi, prosessiparannus

Meriteollisuuden järjestelmien kasvava kompleksisuus, digitalisaatio, integraatio ja automaatio asettavat koko meriteollisuudelle uusia kyberturvallisuusvaatimuksia. Tämä työ tutkii teollisuudenalaa ohjaavia uusimpia kyberturvallisuusjulkaisuja, mukaan lukien eri standardisointi- ja meriteollisuuden organisaatioiden sekä luokituslaitosten teoksia. Tutkimuksen tavoite on parantaa ja yhdenmukaistaa meriteollisuuden sähkö- ja automaatioratkaisuja toimittavan globaalin yrityksen projektiprosessia kyberturvallisuuden näkökulmasta.

Tutkimus koostuu kahdesta osasta: kirjallisuus- ja teollisuuskäytäntöjen katsauksesta ja käytännön osasta, joka tähtää niiden avainosa-alueiden identifioimiseen, joista yritys voi aloittaa projektiprosessinsa parantamisen kyberturvallisuuden osalta. Kirjallisuuskatsaus demonstroi alan valtaapitävän lähestymistavan kyberturvallisuuteen: kokonaisvaltaisen kyberriskien hallinnan organisaation joka tasolla. Kirjallisuuskatsausta käytettiin teoreettisena viitekehyksenä työn empiiriseen osaan, joka perustuu yrityksen eri paikallisia liiketoimintayksiköitä edustavien asiantuntijoiden kanssa toteutettuihin työpajoihin.

Tutkimus tarjoaa metodologian prosessin globaaliin yhdentymiseen, listan havaituista puutteista tämänhetkisessä projektiprosessissa kyberturvallisuuden osalta sekä parannusehdotuksia näihin. Yritys parantaa kaikkia listan kohteita, mutta priorisoi neljä avainosa-aluetta: puutteet kyberturvallisuuden infrastruktuurissa ja standardoidussa projektiprosessissa, koulutus, konfliktit globaalin ja lokaalin ohjeistuksen välillä sekä kyberturvallisuuden tekniset ratkaisut ja toimintatavat. Työn tuloksena yritys alkoi parantaa globaalia alustaa kyberturvallisuuteen liittyvän tiedon jakamiseen, täydentämään koulutustaan globaalisti päteväksi, selventämään globaalin ja lokaalin ohjeistuksen välisiä ristiriitoja ja kehittämään uutta kyberturvallisuuden palveluratkaisua.

Kokonaisuutena työ tarjoaa lukijalle yleiskatsauksen meriteollisuuden kyberturvallisuuden nykytilanteeseen ja auttaa valmistautumaan tulevaisuuden vaatimuksiin. Työ esittää myös käytännön ehdotuksia kyberturvallisuuteen liittyviin ongelmiin, joita yrityksen projektiorganisaatio kohtaa. Työn aikana aloitettuja kehitysprosesseja jatketaan linjassa yhtymätason turvallisuuspolitiikan globalisoinnin kanssa.

PREFACE

The fascinating topic for this research and the pleasant environment for carrying it out were offered by ABB Marine & Ports Oy. I would like to thank the company, the examiner Jose Luis Martinez Lastra from Tampere University of Technology and the instructor Olli Huttunen from ABB Marine & Ports Oy for supporting me through the process.

I would like to express my special appreciation and thanks to Sami Laine, Ahmed Hassan, Yago Parrondo, Kees van Overveld, Jaime Caserza Bovero, Andrea Crosetti and Massimo Siani from the ABB Group – without your input, completing this thesis would have been impossible. I also want to send a common thanks to everyone else from the company sharing their valuable knowledge with me during the work.

Finally, I would like to thank my family for supporting me through my studies and my friends for always being there for me.

Helsinki, 17.11.2017

Riikka Peura

CONTENTS

LIST OF SYMBOLS AND ABBREVIATIONS

ABB	Asea Brown Boveri
ABS	American Bureau of Shipping
AIS	Automatic identification system
AMEA	Asia, Middle East and Africa
ARBD	Assessment of Risk Based Design
ARPA	Automatic radar plotting aid
BIMCO	Baltic and International Maritime Council
CC	Common Criteria (ISO/IEC 15408 standard)
CCC	Certificate of Cyber Compliance (by ABS)
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT	Computer Emergency Response Team
CFR	Code of Federal Regulations (of the United States)
CIA	Confidentiality, integrity and availability
CIAA	Confidentiality, integrity, availability and authenticity
CIS	Centre of Internet Security
CiSP	Cyber Security Information Sharing Partnership
CMS	Cybersecurity Management System
CMSC	CyberSafety Management System Certificate (by ABS)
CRMP	Cyber Risk Management Program
CSA	Cyber Security Assessment
CSC	Critical Safety Control
CSCG	Focus Group on Cybersecurity (of CEN-CENELEC)
CSO	Company Security Officer
CSP	Cyber Security Plan
CySO	Cyber Security Officer
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security (of the United States)
DMAIC	Define, Measure, Analyze, Improve and Control method of Six Sigma
DNV	Det Norske Veritas
DoS	Denial of Service
DPS	Dynamic positioning system
ECDIS	Electronic chart display and information system
ENISA	European Union Agency for Network and Information Security
EU	European Union
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Act
GL	Germanischer Lloyd
GNSS	Global navigation satellite system
GPS	Global positioning system
HCD	Human-Centred Design
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IMO	International Maritime Organization
ISM Code	International Management Code for the Safe Operation of Ships and for Pollution Prevention

ISO	International Organization for Standardization
ISPS Code	International Ship and Port Facility Security Code
ICT	Information and communications technology
ISA	International Society of Automation
ISACA	Information Systems Audit and Control Association
ISF	Information Security Forum
IT	Information technology
JTC1	First Joint Technical Committee of ISO and IEC
LR	Lloyd's Register
MSC	Marine Service Center
MTSA	Maritime Transportation Security Act
MTS	Maritime Transport System
NIST	National Institute of Standards and Technology
OT	Operational technology
PDCA	Plan-Do-Check-Act
RF	Radio frequency
SCM	Security Continuous Monitoring
SL	Security Level
SMS	Safety Management System
SOC	Security Operations Center
SSA	Ship Safety Assessment
SSP	Ship Safety Plan
USB	Universal Serial Bus
USCG	United States Coast Guard
VDR	Voyage data recorder
VOIP	Voice over IP

hr	hour
Kb	Kilobyte
Mb	Megabyte
min	minute

.

1. INTRODUCTION

The world of bits, also known as cyberspace, is an inseparable part of today's world. The global economy, security of the society, business activities and everyday life increasingly rely on the successful and safe operations in the cyberspace. Digitalization offers nearly unlimited opportunities when the geographical and timely boundaries diminish their significance. At the same time, the vulnerability grows. When the meaning of bits compared to physical atoms is growing, the importance of considering the safety of cyberspace is also increasing. Cybersecurity is not only a technological, but a strategic and political issue which touches everyone and which everyone for their part is responsible for. The maritime sector has awakened to this transformation – previously not so cyber reliant industry now has to adapt to the changes that are inevitably coming. (J. Limnéll et al. 2014, p. 13-14)

The increasing complexity, digitalization, integration and automation of systems that the maritime industry relies on requires holistic cyber risk management onboard. More frequently, different systems are also networked together and connected to the internet, which grows the cyber risk (The Guidelines on Cyber Security Onboard Ships 2017, p. 5). Cybersecurity is mandatory not only for the protection of data, but for ensuring safe and reliable operations (Recommended Practice – Cyber Security Resilience Management 2016, p. 6). The maritime sector is a vital part of the global economy and must be protected from the safety, environmental and commercial consequences of poor execution of cybersecurity. In the worst case, a cyber incident may lead to loss of life, control of the ship or sensitive data – or the permission of criminality, such as kidnap, theft of cargo or imposition of ransomware, for example (H. Boyes & R. Isbel 2017, p. 4).

The use of new technologies may provide improved efficiency and safety but also grows cyber risk. In order to achieve and fully embrace the benefits, cybersecurity needs to be considered on all levels of the organization and organizations need to establish and follow a solid cyber strategy. A large part of security breaches is caused by people and poor processes which means that also personnel, physical and physical aspects related to the technological maritime systems need to be considered when assessing the cyber risk (H. Boyes & R. Isbel 2017, p. 12). At its best, by demonstrating best cybersecurity practices, the organization may develop cybersecurity as competitive advantage to increase its market share and to achieve the position of market leader. Cybersecurity provides new business opportunities when for example new offerings such as cybersecurity products and services are released to the market. The maritime industry, despite its slightly slower pace, is also in the middle of this transformation.

1.1 Background

Increasing requirements regarding cybersecurity during the whole lifecycle of a project are forcing organizations to evaluate and re-scan their operations on all levels, starting from the management. To be able to follow the constantly updating standards, rules and regulations of the industry, anticipation and a look to the future is needed. Some of the current recommendations and best practices might not be requirements yet, but companies must be prepared for the transformation from recommendations to rules to happen soon in the future. To answer this need, a literature review of the newest cybersecurity publications of the maritime industry setting the future trend is provided in this thesis.

Another challenge organizations are facing is the nature of global business. Wide networking is a norm, but geographically widespread business units, customers and other stakeholders cause challenges when forming and trying to follow common policies and procedures. The impact of cultural differences and diverse organizational cultures cannot be forgotten, either. It has also been noticed, that different stakeholders react to cybersecurity in a very different way – some of them have recognized the importance of it and have their own, quite solid and active ways to work, taking into account cybersecurity related issues diversely while others still have plenty of room for improvement in their actions.

ABB (Asea Brown Boveri) Marine & Ports business unit, specifically the marine business area and from now on referred to as ABB Marine, has recognized the need to align and unify their process and standardize procedures related to cybersecurity during the phases of their projects. In an ideal situation, different local business units would follow the same, common cybersecurity execution and maintenance process for projects. Due to the local nature and relative independence of different units, this kind of aligning of processes is a challenge. In order to move towards more global processes, it is required to investigate the already existing process and procedures in different local business units and to collect together the best cybersecurity practices. With the help of the findings of this investigation, it is possible to identify the key areas of focus from which to begin the unification of processes.

1.2 Research questions and objectives

The research question set for this study is:

- How a global company on the marine business, like ABB Marine, can improve its project execution process incorporating cybersecurity components?

The aim and objective of this study is to improve the cybersecurity project execution process of ABB Marine in two ways. One goal is to provide an overall picture of the

current cybersecurity trends of the maritime industry and to compare those to ABB Marine's operations by identifying any improvement areas in ABB Marine's cybersecurity requirements and cybersecurity project execution process. Another, practical goal of the work aims at global unification of the cybersecurity project execution process of the company. This process is started by first prioritizing the implementation order of the identified improvement areas – by identifying the key areas of focus. Thus, the research question breaks down into the following questions:

- What kind of approach to maritime cybersecurity do the latest literature and industrial practices take?
- What kind of best practices are already performed in different local business units of the company?
- Which best practices are worth implementing globally considering the cost benefit ratio?

The mechanisms used for answering these questions are introduced in the chapter "1.4 Methods and structure of the work" of this thesis.

1.3 Perspective and scope of the study

The research is done from the perspective of a project engineer and it focuses on cybersecurity execution during a project process – it is not desired to dig too deep into the technical details of the implementation of cybersecurity described in the literature sources. The study aims to give the reader a general picture of which organizations influence the development of cybersecurity best practices of ABB Marine and how these actors approach the topic of cybersecurity. These approaches are introduced in the literature and industrial practices review.

The reference resources of the literature and industrial practices review section were chosen with the help of experienced employees of ABB Marine. One of the goals was to find relevant stakeholders that have published anything relatively new, defined during the last few years, and specifically related to maritime cybersecurity. The fact that not all the relevant stakeholders have published such releases limits the amount of the literature sources. For example, it was not considered necessary to include every single existing classification society's rules and regulations in the review since they follow the general, in the beginning of the review introduced international and industry neutral standards.

1.4 Methods and structure of the work

This research was conducted as a qualitative study aiming to understand the current state of cybersecurity in the maritime industry and to identify the improvement areas in ABB Marine's cybersecurity project execution process, policies and procedures. To be able to answer the research question of this study, a review of current cybersecurity publications

by relevant sources, including international standards, organizations of maritime industry and classification societies is completed. Also, a series of workshops with cybersecurity responsible persons from different local business units is done in order to find out existing best practices and improvement areas and to collect practical observations.

Theory, which is presented in the literature and industrial practices review, was collected together and used as a basis for the research and to demonstrate what is already published about this topic. The literature and industrial practices review serves as a theoretical framework and also supports the interpretation in the analysis. Inductive reasoning was used to make conclusions based on the findings from the theory and this new information was used to complement the procedures of the company – leading to the identification of key areas of focus for the cybersecurity process unification for projects. As mentioned above, the literature resources were chosen together with the experienced employees of the company to ensure the appropriate size of the sample. The amount of sources cannot be too excessive to ensure a thorough research but it must be comprehensive enough to cover all the relevant stakeholders of the company. Criteria used when selecting the literature resources includes:

- date of publication – as current as possible, preferably after 2012
- connection to maritime industry – as industry specific as possible
- relation to ABB Marine & Ports – significant stakeholders or potential future influencers
- geographical coverage – publications from all the operative regions of ABB.

The findings of the literature and industrial practices review are compared to ABB Marine's cybersecurity requirements and cybersecurity project execution process in order to evaluate the compliance and to enable the identification of any improvement areas. Additionally, empirical examining of the process and current cybersecurity procedures of different local business units of the company, as well as analysis of customer needs and expectations is required. In order to achieve this, the data collection is supplemented with information gathered through cooperation and discussions with responsible persons of the project organization from different local business units. These business units are located in Norway, the Netherlands and Italy. The information gathering is implemented in a form of workshops. For the first workshop, the writer traveled to ABB Marine & Ports, Norway. The rest of the workshops were implemented via telephone.

The aim of the discussions and especially the visit to ABB Marine & Ports, Norway was to learn the project execution process from the perspective of cybersecurity and to find any best practices to share with other business units globally. The contents of the workshop in Norway were analyzed with the cybersecurity responsible persons of ABB Marine & Ports, Finland. The workshop in Norway also provided a chance for open exchange of ideas between different actors. The outcome of the workshop and its review in Finland

were complemented with the views of cybersecurity responsible persons from the Netherlands and Italy. As a result and with the help of the summarized information gathered through actions presented above, the key areas of focus for the beginning of the process unification can be identified.

The study manages the above mentioned items in the following structure: the first section introduces the reader to the topic, the motivation and justification of the research, the research questions and objectives, methods and the research environment of the study, as well as the concept of cybersecurity specifically related to the maritime industry. The second section first clarifies the hierarchical governance relations of different organizations acting in the maritime sector related to cybersecurity and then moves on to reviewing the cybersecurity documents published by these relevant organizations. In the third section, methodology for the process unification is first introduced for other companies to replicate and adapt. After this, the contents of the workshops and the analysis of customer needs and expectations are presented. Based on previous findings, the cybersecurity project execution process improvement area detection is done and suggestions for improvement are stated. Finally, the key areas of focus for the beginning of the process unification are selected and additional future suggestions are provided. In the last section, conclusions are presented including the key findings and results of the research, evaluation of the results and potential future research topics.

1.5 Research environment

This research was conducted at the company ABB Marine & Ports Oy for its Marine business area in Helsinki, Finland. The company is a local business unit of the multinational automation and power technology group ABB's Industrial Automation division. Additionally, ABB group has three other divisions: Robotics and Motion, Electrification Products and Power Grids. Globally, ABB Marine & Ports has 1700 employees in twenty countries and twenty Marine Service Centers (MSC). In total, ABB group employs around 132 000 people in one hundred countries in three operative regions: Europe, the Americas and Asia, Middle East and Africa (AMEA). In 2016, ABB group's revenue was 33 828 million dollars. (ABB 2017a)

ABB Marine & Ports Oy develops electrification and automation solutions for the maritime industry and is globally responsible for ABB's development of the maritime industry solutions. It provides electric propulsion system, trademarked Azipod®. The Azipod solution can be used in different types of vessels such as ice breakers, cruise ships, yachts and tankers to improve their fuel economy, energy efficiency and maneuverability. The savings in fuel consumption are based on the undisturbed water flow in the propellers of the vessel. In an Azipod propulsion system, the control unit rotates 360 degrees and this way enables more accurate maneuvering and increases safety. Additionally, the Azipod system reduces noise production and saves machinery space. The organization of ABB Marine & Ports Oy consists of three parts – propulsion solutions, electrical solutions and

digital solutions project organizations. Additionally, a marine service organization which focuses on the commissioning and maintenance of vessels, exists. (ABB 2017b)

The propulsion solutions organization is specialized in the Azipod propulsion products. The electrical solutions project organization is in charge of delivering the power generation and distribution systems for vessels. The automation project organization delivers integrated marine automation, including the vessel information and control systems, software and analytics. Since ABB Marine & Ports Oy is strongly involved in the full lifecycle of the product, beginning from sales, through planning, design and engineering until the commissioning, maintenance and upgrade, the company is strongly responsible for successful cybersecurity execution during all the project phases. To ensure this, ABB Marine & Ports deploys cybersecurity requirements for three areas: product, project and service. Additionally, requirements for suppliers are presented. This thesis focuses on cybersecurity from the project execution aspect. Figure 1 illustrates the phases of a typical project of ABB Marine & Ports and locates the focus of this study.

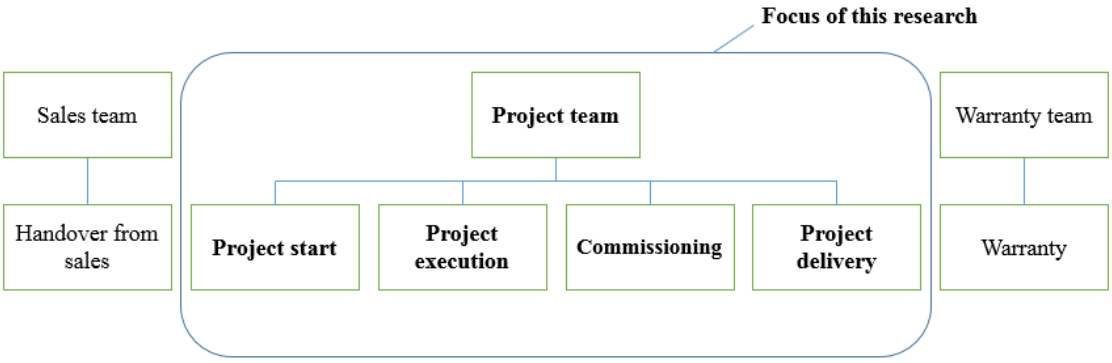


Figure 1: Phases of a typical ABB Marine & Ports Oy project

The evolution of power and automation requires careful consideration of cybersecurity from today's companies, including ABB Marine & Ports. "Modern automation, protection and control systems are highly specialized information technology systems" (ABB 2016) using commercial off the shelf components and standardized communication protocols. Additionally, the systems are distributed and highly interconnected, use storage media and communicate with external systems. This way, the potential attack surface compared to isolated systems increases. The fact that over 50 % of the ABB offering is software-related is a clear demonstration of why cybersecurity is seen as an important issue. Also, compared to "traditional" information technology (IT), power and automation technology has different characteristics and requirements. While IT aims at protecting information from disclosure or financial loss, the main security objective being confidentiality and privacy, power and automation technology protects physical processes focusing on safety, health, environment and finance. The main security objectives of power and automation technology are availability and integrity – the availability requirement of the system may be as high as 99,999 %. A notable difference between IT and

power and automation technology systems is also their lifetime: for IT systems, the system lifetime is approximately 3-10 years while power and automation technology systems may be in use for 5-25 years. (ABB 2016)

ABB Marine & Ports Oy has also recognized proper execution and demonstration of cybersecurity as a way of gaining competitive advantage. Since the maritime industry's cybersecurity awareness and execution levels are not very developed yet, it is a good time to act now and aim at the forerunner and market leader position. When the company can clearly demonstrate its compliance with the newest cybersecurity frameworks, best practices and standards to its customers, it acts as an effective proof of advanced cybersecurity maturity of the company. This may also provide new opportunities and customers, especially when the company can offer new cybersecurity products and services.

1.6 Definition of cybersecurity

This chapter and its subchapters explain the core concepts of cybersecurity to help the reader understand the more detailed approaches in the following second chapter, literature and industrial practices review of this thesis. The categorizations, tools and elements presented in this chapter ease the perceiving of the complete cyber risk management process and they are mutual for several approaches reviewed in the second chapter of this thesis.

No single, comprehensive definition for cybersecurity exists. Cybersecurity can be considered as the operations that the organization carries out to protect itself from cyber attacks and their consequences and the necessary countermeasures the organization takes (M. Lehto & A. Kähkönen 2015, p. 9). According to Lehto and Kähkönen, risk and threat analysis serves as the foundation of cybersecurity, since the structure and elements of the organization's cyber strategy and cyber program rely on these assessed risks and threats. Development of a cyber strategy and cyber program are primary steps for the organization in order to holistically consider its cybersecurity. Cybersecurity can also be considered to base on the identification of the "world of bits", also known as cyber space, as new operational domain and environment (Cyber Strategy 2015, Definition of Cybersecurity 2016).

Increasing cybersecurity can be done by lowering the cyber risk. Emphasis on safety related systems, such as critical infrastructures, is given. A risk-based approach and holistic risk management is the key for an organization to achieve this goal. Cyber risk management can be defined as "the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders" (Guidelines on Maritime Cyber Risk Management 2017, p. 5). The implementation of cybersecurity begins from the management level and requires commitment on all the levels of the organization, since the impact of the human factor on cybersecurity is significant. Improving cybersecurity requires development of an Information Security Management

System (ISMS) and continuous improvement processes such as the implementation of Plan-Do-Check-Act (PDCA) cycle or the Define, Measure, Analyze, Improve, Control (DMAIC) method of Six Sigma, as the information security standard ISO/IEC 27001:2013 (2013) advises.

1.6.1 Maritime industry specific characteristics and threats

The growth of interconnected control systems is a significant factor for the organizations of the maritime industry to consider. The information and operational technology systems of vessels are more increasingly networked not only together but also connected to the internet. Ship or platform systems, such as propulsion plant and ship control and ballast and cargo management combined to digital accesses, for example web-based systems and remote access methods, enable the appearance of new threats such as malware, phishing and vishing (voice phishing) and poisoned links or attachments (J. Jorgensen 2016, p. 7). In the maritime industry, third-party access to the marine systems and more generally to the organization's important assets and third-party service providers are also common. These factors add cybersecurity related requirements of the organization and requirements are also targeted to the organization's stakeholders. Safety critical systems are prioritized when assessing and mitigating the cyber risk.

Cyber risk assessment begins with the identification of cyber threats, which can be either external or internal. The fact that historic evidence is not available and recording of incidents is not required is a challenge of cybersecurity – definitive information about incidents and their impact is absent. However, the organization needs to consider all the aspects of their operation that may increase their vulnerability to cyber incidents. Actors searching these vulnerabilities may be organizations or individuals with different motives, for example:

- activists seeking reputational damage through destruction of data,
- criminals chasing financial gain through selling stolen data,
- opportunists desiring challenge of getting through cybersecurity defences,
- states/state sponsored organizations and terrorists pursuing political gain through disruption to economies and critical infrastructures (adapted from The Guidelines on Cyber Security Onboard Ships 2017, p. 10).

Additionally, the organization's personnel may intentionally or unintentionally compromise cyber systems and data. The organization needs to consider the possibility of human errors when operating and managing the systems of the vessel and the failure of following the technical and procedural protection measures, as well as employees trying to intentionally damage the organization. (The Guidelines on Cyber Security Onboard Ships 2017, p. 11)

Cyber attacks can be divided to two categories: targeted and untargeted attacks. In targeted attacks, the organization or the vessel's systems and data are the intended target and in untargeted attacks, they are one of many targets. In Table 1, some of the typical tools and techniques used under these circumstances are presented (The Guidelines on Cyber Security Onboard Ships 2017, p. 11-12):

Untargeted attacks	**Targeted attacks**
Malware: malicious software to access or damage a computer without the knowledge of the owner	Brute force: trying all the possible passwords systematically hoping to eventually find the correct one
Social engineering: a non-technical technique used to manipulate the organization's personnel to brake a cybersecurity procedure for example through interaction in social media	Denial of Service (DoS) and Distributed Denial of Service (DDoS): flooding the network with data to prevent the legitimate users from accessing information, in DDoS multiple servers/computers are taken under control
Phishing: emails targeted to a large number of people requesting sensitive or confidential information or a visit to a fake website	Spear-phishing: emails targeted to a specific person, often containing malicious software or links
Water holing: a fake website or compromising an authentic website to exploit visitors	Subverting the supply chain: compromising software, equipment or supporting services necessary to the targeted organization/vessel
Scanning: attack randomly targeted to a large portion of the internet	

Table 1: Typical tools and techniques of cyber attacks (The Guidelines on Cyber Security Onboard Ships 2017, p. 11-12)

According to DNV GL (Det Norske Veritas, Germanischer Lloyd), there are four possible responses to a cyber risk or threat: avoid, reduce, accept or transfer. Avoidance means circumventing the risk "by changing the course of action". Reducing the risk requires implementing "corrective actions to reduce the likelihood and/or the severity". Through acceptance of a risk, it simply is accepted and a chance of negative impacts is taken. Transferring the risk means outsourcing of it through sharing it with third parties, which means for example cyber insurances. (Recommended Practice – Cyber Security Resilience Management 2016, p. 29)

There are several reasons for the importance of the cybersecurity of vessels and the growing interest in cyber. According to H. Boyes and R. Isbell, a vessel is "a complex cyber-physical engineered system that encompasses both waterborne activities and systems, and remote elements such as navigation signals" and it contains five main asset types – "plant and machinery, operational technology, information technology, radio frequency (RF) communications and navigation systems" (H. Boyes & R. Isbell 2017, p. 19). Boyes and Isbell state, that a loss or compromise of these assets may have impact upon

- "the health and safety of staff and other people…
- the ability of the ship to operate safely and to not endanger other ships, maritime structures or the environment; and
- the speed and efficiency at which the ship can operate" (H. Boyes & R. Isbell 2017, p. 19).

With effective cybersecurity execution, these scenarios can be avoided. At its best, operating on cyber domain may provide the organization with multiple benefits. Lloyd's Register lists some reasons for the increased interest in cyber, including:

- "the potential for better business performance"
- "the ability to capture and analyze a wide range of data, including operational, service, monitoring, regulation and off-ship storage data"
- "the ability to easily update products based on software…"
- "the ability to integrate, flexibility control and optimize systems"
- "the potential for better communication both on and off ship (for example, for data sharing and performing updates and maintenance)" (Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping 2016, p. 3).

1.6.2 Information and operational technology systems

When considering cybersecurity of a vessel, it is necessary to make a distinction between information and operational technology systems. According to the Guidelines on Maritime Cyber Risk Management by International Maritime Organization (IMO), information technology systems concentrate on the use of data as information while operational technology (OT) systems focus on the use of data to control or monitor physical processes (2017, p. 4). The protection of information and data exchange between information and operational technology systems is also an important factor to be considered.

The development of new technologies causes the fact that IT and OT systems onboard ships are increasingly networked together and furthermore connected to the internet. The Baltic and International Maritime Council (BIMCO) points out that this connectivity together with digitalization, integration and automation reliance of systems increases cyber risks onboard – for example in the form of unauthorized access or malicious attacks to

ship's systems and networks. (The Guidelines on Cyber Security Onboard Ships 2017, p. 5)

Lloyd's Register's (LR) Guidance Note "Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping – Lloyd's Register's Approach to Assurance" states that connected systems transform the vessel into a total system of interlinked systems – "a system of systems" (2016, p. 4). Such vessels can be described with a new term, "cyber-enabled". According to LR, cyber systems do not exactly substitute traditional electro-mechanical systems and operators but enable combining traditional elements with more complex behavior. At its best, a cyber-enabled vessel can increase its efficiency and safety through improved monitoring and communication. Using the latest information and communications technology (ICT), it is also possible to enhance safety, reliability and business performance, but at the same time the number of risks increases (Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping 2016, p. 1). LR suggests that these risks must be identified, understood and mitigated to ensure safe integration of technologies into ship design and operations.

Adapted from BIMCO's Guidelines on Cybersecurity Onboard Ships and LR's Guidance Note, onboard systems include, but are not limited to:

- **Bridge & navigation systems:** Navigation systems are increasingly digital and networked with interfaces to shoreside networks. Use of removable media for updating of systems may make bridge systems that are not connected equally vulnerable to cyber attacks. Systems in this category are for example electronic chart display and information systems (ECDIS), global positioning systems (GPS), dynamic positioning systems (DPS), global navigation satellite systems (GNSS), automatic identification systems (AIS), voyage data recorders (VDR) and Radar/Automatic radar plotting aid (ARPA).
- **Cargo management systems:** Digital cargo management and control systems may have interfaces to multiple systems ashore. For example shipment-tracking tools available via internet connection expose data in cargo manifests and cargo management systems to cyber risks.
- **Communications systems:** Internet connection via satellite and other wireless communications, including radio communications (broadband, Voice over IP (VOIP)) potentially increase the vulnerabilities onboard.
- **Control systems:** Digital control and monitoring systems for electro-mechanical systems, including main engine, generators, ballast tank, life support, fuel and oil pumps, water tight doors, fire alarms and controls, cargo hold fans, environmental controls, propulsion and steering of the vessel, are vulnerable to cyber attacks. Remote condition-based monitoring and diagnostics increase the risk, as well as integrating these systems to navigation and communications on ships which use integrated bridge systems.

- **Access control systems:** Such systems are used for supporting access control in order to ensure physical security and safety of the vessel and its cargo – including surveillance, shipboard security alarm and electronic ”personnel-on-board” systems.
- **Charterer equipment:** Charterers may use equipment, for example sonar and seismic survey systems, wireless access points, IP ports and wireless phones, which increase cyber vulnerabilities.
- **Passenger servicing and management systems, public networks:** Valuable data related to the passengers may be held by digital systems used for property management, boarding and access control. Intelligent devices, such as tablets and handheld scanners, can act as attack vectors when the collected data is transmitted to other systems. Fixed and wireless networks with internet connection, for example for guest entertainment use, should be considered uncontrolled and held segregated from safety critical systems of the vessel. Onboard networks used for administration of the vessel or the welfare of the crew, as well as software provided by ship management companies or owners, belong to the same category. (Guidelines on Cyber Security Onboard Ships 2017, p. 14-15; Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping 2016, p. 4)

1.6.3 Safety and security

In addition to the distinction between IT and OT systems, cybersecurity can be considered from two points of view – safety and security. Both cybersecurity and cybersafety have an effect on the safety of the vessel, not only on the ship itself but the personnel onboard and the cargo (Guidelines on Cyber Security Onboard Ships 2017, p. 6). According to the definition of BIMCO’s Guidelines on Cyber Security Onboard Ships (2017, p. 6), cybersecurity concentrates on protecting IT, OT and data from unauthorized access, manipulation and disruption while cybersafety manages the risks from the loss of availability and integrity of safety critical data and OT.

BIMCO’s Guidelines on Cyber Security Onboard Ships (2017, p. 6) introduce several examples of situations, where cybersafety incidents arise. For example the corruption of chart data held in an ECDIS is a cybersecurity incident, which affects the availability and integrity of the OT and this way endangers cybersafety. Other examples presented by BIMCO are failures during software maintenance and patching and the loss of or manipulation of sensor data critical for the operation of the vessel. These examples indicate, that the causes of a cybersafety incidents may be different from those of cybersecurity incidents and effective cybersafety and cyber risk management with training and awareness of company procedures and policies is necessary in both cases.

The Focus Group on Cybersecurity (CSCG) of The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization

(CENELEC) deepen the definition of cyber security in its document "Definition of Cybersecurity" (2016) by dividing security to five domains: Operations, Information, Communications, Physical and National Security. By Communications Security, CEN-CENELEC means the "protection against a threat to the technical infrastructure of a cyber system" which may make the system incapable of performing its original intended activities. Physical Security focuses on prevention of physical threats, such as physical access to a server or insertion of malicious removable media into a network, which influence the well-being of the system. National Security takes the potential drive for political, military, or strategic gain of the attacker into consideration. (Definition of Cybersecurity 2016, p. 13)

1.6.4 Confidentiality, integrity and availability model

National Institute of Technology and Standards (NIST) presents a categorization for information and information system security in its Federal Information Processing Standards (FIPS) Publication Series, Publication 199 (2004). This categorization is often referred to as confidentiality, integrity and availability (CIA) security model and it can be exploited when assessing the impact of cybersecurity incidents caused by different sources.

Federal Information Security Management Act (FISMA) of 2002 names confidentiality, integrity and availability as the three security objectives for information and information systems. Confidentiality is defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" (44 U. S. Code, Section 3542). Integrity means "guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" while availability is defined as "ensuring timely and reliable access to and use of information…" (44 U. S. Code, Section 3542).

BIMCO names three situations in its Guidelines on Cyber Security Onboard Ships (2017, p. 19), where the CIA model can be applied during the assessment of the impact of:

- loss of confidentiality – a disclosure of ship, crew, cargo and passenger related information or data and unauthorized access to these sources
- loss of integrity, which can lead to endangering the safe and efficient operation and administration of the vessel through information and data modification and destruction
- loss of availability, caused by the destruction of the information or data or the disruption to services or operations of the systems of the vessel.

The importance of the three factors – confidentiality, integrity and availability – is related to the type of the system in question, mostly whether it is an IT or OT system. The use of the information or data varies and so does the relative importance of the factors. BIMCO's

Guidelines on Cyber Security Onboard Ships (2017, p. 19) mention two examples of the different division of the importance of these factors. When assessing the vulnerability of OT systems onboard ships, especially safety critical systems, the priority is to focus on availability and integrity instead of confidentiality. Even a small loss of data availability can lead to fatal consequences. On the other hand, when assessing the vulnerability of commercial operations related IT systems, confidentiality and integrity are in the focus instead of availability – moderate delays in the availability of data usually cause no risks.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) add one more 'A' to the CIA model in their standard 27000:2014 (2014) – authenticity. According to this confidentiality, integrity, availability and authenticity (CIAA) model, authenticity can be defined as "the property that an entity is what it claims to be". As clarified above, the importance of these security properties can be higher or lower. DNV GL states, that in order to be able to define the levels of importance of these properties for any safety critical system, evaluation of consequences of a breach of the property is necessary (Recommended Practice – Cyber Security Resilience Management 2016, p. 24). Typically, the impact levels are categorized as high, medium and low. DNV GL presents typical questions to help assessing these consequences and the importance of the property in the following way:

- **Confidentiality:** How important is the fact that this information is and remains confidential? What are the consequences of disclosing this information?
- **Integrity:** How critically this information needs to be complete and exact? What are the consequences of this information being wrong or altered?
- **Availability:** What are the consequences of this information/system being unavailable for 5 min/30 min/1 hr/1 day?
- **Authenticity:** How important is it to be sure, that the source of information is who it claims to be? (Recommended Practice – Cyber Security Resilience Management 2016, p. 25)

Additional properties, such as reliability, non-repudiation and accountability, can also be added to the assessment model, but confidentiality, integrity and availability are the most commonly handled properties. Table 2 presents the potential impact levels – high, medium and low – of the CIA model and describes the nature of the consequences of a security breach on each level:

Impact level	**Definition**	**Consequences in practice**
Low	Loss of CIA(A) property: **limited** adverse effect on company, ship, organizational assets or individuals	A security breach might: i) cause a degradation in ship operation to an extent and duration that primary functions can still be performed but their effectiveness is *noticeably* reduced; ii) cause minor

		damage to assets; iii) result in minor financial loss; or iv) result in minor harm to individuals.
Medium	Loss of CIA(A) property: **substantial** adverse effect on company, ship, organizational assets or individuals	A security breach might: i) cause a *significant* degradation in ship operation to an extent and duration that primary functions can still be performed but their effectiveness is *significantly* reduced; ii) cause *significant* damage to assets; iii) result in *significant* financial loss; or iv) result in *significant* harm to individuals, excluding loss of life or serious life threatening injuries.
High	Loss of CIA(A) property: **severe** or **catastrophic** adverse effect on company, ship, organizational assets or individuals	A security breach might: i) cause a *severe* degradation in or loss of ship operation to an extent and duration that one or more primary functions cannot be performed; ii) cause *major* damage to assets; iii) result in *major* financial loss; or iv) cause *severe* or *catastrophic* harm to individuals, including loss of life or serious life threatening injuries.

Table 2: Impact levels using CIA model (adapted from Guidelines on Cyber Security Onboard Ships 2017, p. 20)

1.6.5 Human factor

The effect of the human factor on cybersecurity cannot be understated. The human element plays a significant role in the majority of cyber security incidents (Recommended Practice – Cyber Security Resilience Management 2016, p. 8). Due to the high level of the system connectivity and integration, even small human errors for example by a system operator may have serious consequences. Cybersecurity awareness and competence building among the staff is extremely necessary also in order to avoid incidents caused by for example social engineering or external workers allowed in the facilities, not forgetting the possibility of insider threat or unintentional errors.

When considering cybersecurity, a holistic approach is mandatory. The onion model is an effective way to describe the importance of the human factor on cybersecurity. For example, disabling unnecessary Universal Serial Bus (USB) ports of a laptop may be a

technical control method to ensure cybersecurity – it reduces the chance of inserting malicious external devices into the laptop. The laptop can be thought to be located in the center of an open cut onion. The laptop is located in a cabinet, which represents the next layered shell of the onion. The cabinet is located in a room, which is inside a vessel, which represent the next layers of the onion. The access from one layer to another is secured – for example, only authorized people are allowed in the vessel and further on, only authorized people may access the room. Finally, only limited amount of people may have the key to the cabinet. In order to access the USB ports of the laptop, the attacker has to be able to break through all these controls, which are often highly related to the human factor. The attacker may for example be let inside the vessel through social engineering, which is enabled by a human error. On the other hand, in case all the outer layers succeed in their protection measures, the attacker will never gain access to the laptop. In this case, the disabling of unnecessary USB ports only has a nominal meaning. This scenario reflects the importance of planning cybersecurity as a totality, beginning from the highest level.

2. LITERATURE AND INDUSTRIAL PRACTICES REVIEW

In this section, the latest cybersecurity related publications of the selected reference sources are reviewed. Each chapter provides the reader with an overview of the nature of the respective publication, with its most important characteristics and individual approach to the topic of cybersecurity. In the beginning of the section, the levels of governance targeted to ABB Marine & Ports and especially the role of classification societies is explained. After this, each reference is introduced one by one, beginning from the industry neutral ones, entering into maritime industry specific publications and the approaches of classification societies. At the end of this section, potential future influencers' aspects are presented and finally, a summary of the section is provided.

2.1 Levels of governance

As a maritime and shipbuilding industry system supplier, it is required from ABB Marine & Ports to fill multiple requirements coming from different actors and different levels. The levels and typical actors are described in Figure 2. The hierarchy of the actors is directive only in order to provide the reader with a preliminary image of the relations between different actors – in reality, such strict notations cannot be made since these actors work in close cooperation. Both non-governmental and government dependent and international governmental organizations align requirements that ABB needs to meet. The rules and regulations can be set by international standardization organizations or they may be coming from national level, for example. In addition, classification societies of shipbuilding and maritime industry and private sector companies add their own standards to the collection.

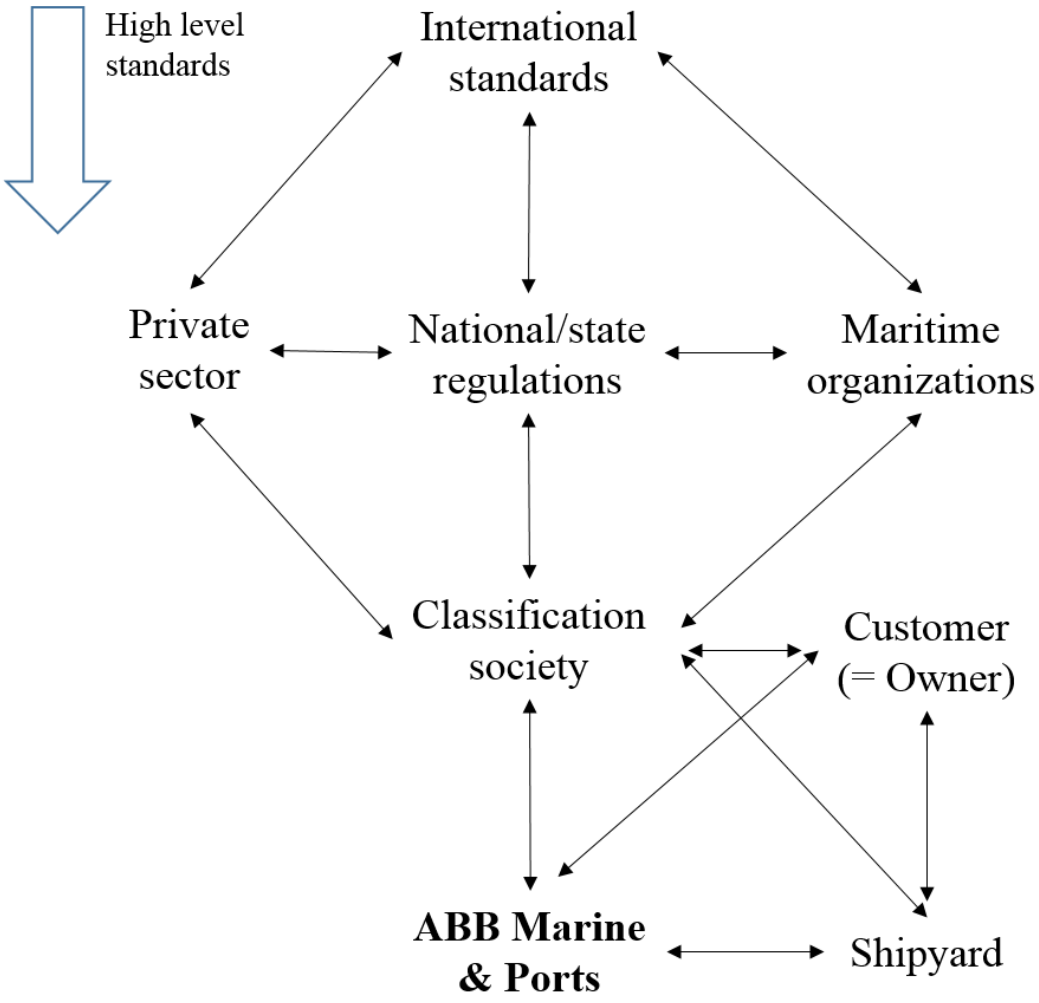


Figure 2: Different actors setting requirements for ABB Marine & Ports

Classification societies, which are non-governmental organizations objectively evaluating vessels, have a close influence on the work at ABB Marine & Ports. They can also work for the state under whose flag the vessel is registered, which connects them to the national level. Some classification societies also cooperate with private sector companies and do research in order to improve their rules and better prepare for the future innovations of maritime industry. Classification societies set out rules and requirements on the safety and security of the vessels based on technical standards. The construction and the operation of the vessel must demonstrate compliance with these standards in order to pass the survey of the classification society. This is why ABB Marine & Ports must follow the regulations of classification societies very strictly. Without an approval of a classification society, a vessel is not allowed to sail and it most likely will not earn an insurance either. Despite giving their approval, classification societies take no responsibility of the conditions, such as the safety or seaworthiness of the vessel during its operation.

Typically, the customer which is also called the owner, purchases a turnkey shipbuilding project from the selected shipyard. In order to deliver the project and to construct the vessel, the shipyard orders different types of products and work from subcontractors.

ABB Marine & Ports works as one of these subcontractors by delivering for example the propulsion system, power plant and automation of the vessel to be constructed. The owner has the authority to choose the inspecting classification society. This way, the owner's decision affects both the work of the shipyard and ABB Marine & Ports when they have to comply with the requirements of the classification society.

2.2 Industry neutral publications

In this chapter, generic industry neutral standards related to cybersecurity are presented. It is noticeable, how they link with each other. The standards in this chapter often take a high-level approach to the concepts of safety and security. Commonly referenced and relevant standards, which the majority of the following frameworks and guides in the literature and industrial practices base on, are produced by the IEC and ISO. Other industry wide recognized frameworks have been published by the previously as the Information Systems Audit and Control Association known organization ISACA, the Information Security Forum ISF and the National Institute of Standards and Technology NIST.

2.2.1 ISO/IEC standards

The ISO/IEC 27000 (2016), also known as the Information Security Management Systems (ISMS) family of information security standards was developed by the sub-committee 27 of the first Joint Technical Committee (JTC1) formed by ISO and IEC and consists of fifteen parts. The collection of standards is growing and it focuses on providing guidance on best practices of information security management. The central concept of the ISMS family of standards is an Information Security Management System which is a part of the overall management system of the organization and managing risks through information security controls. According to the ISO definition, an ISMS is "based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security" in the context of the organization, and "a holistic approach to managing information security – confidentiality, integrity and availability of information and data" (A. Terroza 2015, p. 5). ISO/IEC 27001:2013 (2013) specifies the requirements for such ISMS but is not a technical standard describing the technical details of such system. In addition to information technology, the standard concentrates on important business assets such as resources and processes of the organization. (A. Terroza 2015, p. 8)

Organizations seeking conformance to ISO/IEC 27001:2013 (2013) must meet requirements presented in the form of the following Clauses:

- Clause 4: Context of the organization
- Clause 5: Leadership
- Clause 6: Planning

- Clause 7: Support
- Clause 8: Operation
- Clause 9: Performance evaluation
- Clause 10: Improvement. (ISO/IEC 27001:2013)

The standard also provides a list of fourteen reference control objectives and controls which help the implementation of information security best practices and which are "derived from and aligned with those listed in ISO/IEC 27002:2013" (2013). For example, the objective of "A.5.1 Management direction for information security" is: "To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations" (ISO/IEC 27001:2013, p. 16). To achieve this, for example definition of policies for information security should be completed and they should be approved by the management, published and furthermore communicated to employees and relevant external parties. (ISO/IEC 27001:2013, p. 16)

Another IT security techniques standard published by the JTC1 of ISO and IEC is the ISO/IEC 15408 (2008 & 2009) "Information technology – Security techniques – Evaluation criteria for IT security" or "Common Criteria" (CC) which consists of three parts and presents a general evaluation model for computer security certification. Other commonly recognized cybersecurity related and relevant standards are IEC 62443 (2016) and IEC 61508 (2010) series of standards. IEC 62443 provides guidance on Industrial Automation and Control Systems (IACS) security while IEC 61508 concentrates on the "functional safety of electrical/electronic/programmable electronic safety-related systems" (IEC 61508 2010). The list of cybersecurity related standards presented in this chapter is not exhaustive, but, in the scope of this thesis, sufficient.

2.2.2 COBIT Framework and ISF Standard of Good Practice for Information Security

In 2012, ISACA published a holistic information governance and management framework, COBIT 5, to answer the organizations' needs of keeping risks on an acceptable level, maintaining availability to systems and services and complying with relevant laws and regulations. There is also an online version of COBIT 5, which is mainly available free of charge. COBIT 5 presents five principles and seven enablers, which allow organizations to create optimal value of information technology. The principles of COBIT 5 are meeting stakeholder needs, covering the enterprise end-to-end, applying a single integrated framework, enabling a holistic approach and separating governance from management. The enablers that COBIT 5 lists are:

- principles, policies and frameworks,
- processes,
- organizational structures,

- culture, ethics and behavior,
- information,
- services, infrastructure and applications and
- people, skills and competencies. (ISACA 2012)

In 2016, Information Security Forum (ISF) published "The Standard of Good Practice for Information Security 2016" (the Standard) which fully covers the topics of previously introduced ISO/IEC 27002:2013 and COBIT 5, as well as the following NIST Framework. The topics introduced in the Standard include threat intelligence, cyber attack protection, industrial control systems (ICS), information risk assessment, security architecture and enterprise mobility management. The Standard states to help organizations meet regulatory and compliance requirements, respond to rapidly evolving threats – even sophisticated cyber attacks – and be agile and exploit new opportunities. The Standard presents threat intelligence for increasing cyber resilience and guides how information risks can be managed to an acceptable level. The Standard, however, is available free of charge only for the ISF Members. (Information Security Forum 2016)

2.2.3 National Institute of Standards and Technology Framework

NIST, a measurement standards laboratory and an agency acting under United States Department of Commerce, has noted the importance of cybersecurity related to critical infrastructures and produced already widespread guide, "Framework for Improving Critical Infrastructure Cybersecurity" (2017). The guide is currently published as a Draft Version 1.1 and NIST collects feedback and comments, intending to publish a final version around the fall of 2017. It is likely to become an influential benchmark for any organization for assessing their cybersecurity (L. Shen 2014, p. 2).

The NIST Framework defines critical infrastructures as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of matters", which acts as a decent definition for any other state as well. The Framework, being flexible and technology-neutral, is intended to complement the organization's risk management process and cybersecurity program by providing classification and mechanisms for organizations to answer questions regarding:

- the description of their current cybersecurity posture
- the description of their target state for cybersecurity
- the identification and prioritization of opportunities for improvement, following a continuous and repeatable process
- assessing progress towards the target state

- communication of cybersecurity risk among internal and external stakeholders. (Framework for Improving Critical Infrastructure Cybersecurity 2017, p.8)

The Framework takes a risk-based approach to cybersecurity and consists of three parts: the Framework Core, Profiles and Tiers. The Core presents various cybersecurity related activities and outcomes that can be found in a cybersecurity program and which are organized to five main Functions: Identify, Protect, Detect, Respond and Recover. These functions are divided to Categories and Subcategories which reference to industry-accepted standards and guidelines, Informative References such as ISO, for more specific guidance on how to implement a specific activity or outcome.

For example, when the organization wants to view its protection against cyber threats, it can look at the Protect Function, which is divided to six Categories:

- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology.

These Categories are further divided to multiple Subcategories of cybersecurity activities, for example the Access Control Category has six Subcategories, first of them being "Identities and credentials are issued, managed, verified, revoked and audited for authorized devices, users and processes" (Framework for Improving Critical Infrastructure Cybersecurity 2017, p. 36). This Subcategory is then linked to multiple Informative References including publications of for example the International Society of Automation (ISA) and ISO/IEC.

The Profiles present the outcomes based on business needs that the organization has selected from the Categories and Subcategories. The aim is to align the Functions, Categories and Subcategories with the requirements, risk tolerance and resources of the organization. The Profiles provide a summary of the organization's cybersecurity activities and enables self-assessment when creating a Current Profile and a Target Profile. The Current Profile represents the current state of the organization's cybersecurity program and the Target Profile reflects the goal or target state that the organization desires to achieve. Once both of these Profiles are identified, the organization can identify any gaps between those two and create a roadmap for areas that need strengthening in order for the organization to achieve its target state. To ensure flexibility of implementation, there is no template for creating Profiles presented in the Framework. (L. Shen 2014, p. 2)

The third component of the Framework, the Implementation Tiers, provides the description of the level to which the organization's cybersecurity risk management practices

show the characteristics defined in the Framework. Organization's practices can be characterized over a four-stage range from Partial to Adaptive, Partial representing the lowest level which means that the organization does not follow formalized practices and has little awareness of cybersecurity risk and Adaptive meaning that the organization is capable of adaptive, lessons learned based and predictive cybersecurity management. Once the organization has identified their Tier stage, they can decide whether they should consider moving to a higher stage by investing additional resources, which is encouraged when this move is considered cost effective and improves cybersecurity. (Framework for Improving Critical Infrastructure Cybersecurity 2017, p. 13)

NIST presents four ways in which the Framework can be used – reviewing of cybersecurity practices, establishing or improving a cybersecurity program, communicating cybersecurity requirements with stakeholders and identification of new or revised Informative References. The current cybersecurity activities of the organization can be compared to the outcomes defined in the Core to find out which areas may need to get improved. The Framework also demonstrates steps to follow in order to create a new or improve the current cybersecurity program. Since the Framework defines a common language for communicating cybersecurity requirements, it can be used when communicating with important stakeholders. Finally, the list of Informative References included in the Framework may help organizations to find opportunities to revision or creation of new standards or guidelines. (L. Shen 2014, p. 3)

2.3 International maritime industry specific publications

In this chapter, reference sources specifically connected to the maritime sector are introduced. The publications reviewed in this section are released by the European Union Agency for Network and Information Security, International Maritime Organization, Baltic and International Maritime Council and the Government of the United Kingdom.

2.3.1 European Union Agency for Network and Information Security

The European Union Agency for Network and Information Security (ENISA) published the first ever European Union (EU) report on cybersecurity challenges of the maritime sector: "Analysis of Cyber Security Aspects in the Maritime Sector" (2011). The analysis first points out that the maritime sector is critical for the European society. For example in 2010, 52 % of the goods traffic was carried out by maritime transport while a decade ago this number was only 45 %. ENISA identifies, that the growing ICT reliance of maritime operations also grows the cyber threat menace and the need to ensure the dependability and ICT robustness against cyber attacks is a key challenge. The document focuses on presenting key insights and high-level recommendations of this area, with a touch on

the policy context at the European level. (Analysis of Cyber Security Aspects in the Maritime Sector 2011, p. 6)

The first observation that ENISA introduces is the fact that the awareness level on cybersecurity in the maritime factor is low to non-existent. One of the reasons for this may be that not a lot of cybersecurity incidents within this sector create sufficient media exposure nor are there mechanisms in the Member States of EU to identify and report these incidents specifically within the maritime sector. ENISA recommends the Member States to implement awareness raising campaigns, especially to promote cybersecurity training. The target audience would be all the relevant stakeholders of the maritime sector, for example ship crews and port authorities, and the provision could be coordinated by cybersecurity officers such as national Computer Emergency Response Teams (CERT) and cybersecurity offices. (Analysis of Cyber Security Aspects in the Maritime Sector 2011, p. 13)

ENISA notes, that the use of specific technologies, ICT complexity and the growing connectivity of the maritime systems causes challenges to ensure security provisions. It would benefit all the stakeholders to commit to a common strategy and development of good practices, aiming to ensuring security by design for all the ICT components of the maritime sector. Also cybersecurity aspects should be added to the maritime regulations and policies since they currently only consider the physical aspects of safety and security. In order to achieve this, a holistic risk-based approach with the use of proactive cyber and information security risk management principles is mandatory. (Analysis of Cyber Security Aspects in the Maritime Sector 2011, p. 7)

At last, ENISA's analysis manages the fragmentation of maritime governance context – it is divided between for example international, national and European levels. ENISA suggests that IMO, European Commission and the Member States should aim to harmonize and align international and European policies of this sector. Different roles and responsibilities at various levels should be specified by the Member States. Also the coordination and cooperation between all the stakeholders, such as CERTs and port authorities, should be defined with the help of public-private sector interaction. Improved information exchange would also potentially help insurers to develop their actuarial models, reduce risks and provide better insurance contracts to the stakeholders. (Analysis of Cyber Security Aspects in the Maritime Sector 2011, p. 7)

At the end of ENISA's analysis, suggested next steps are presented:

- **Short-term:** stimulating dialogue and information exchange between maritime and connected stakeholders, raising cybersecurity awareness, developing strategies and good practices defining ICT security requirements
- **Mid-term:** developing cybersecurity trainings, defining roles and responsibilities related to cybersecurity at the European and national levels, taking a risk-based

approach towards cybersecurity and adding considerations towards cybersecurity in maritime sector governing frameworks

- **Long-term:** developing standards and setting regulations in order to achieve cybersecurity, developing information sharing and analysis centres at national and European level, aligning and harmonizing international and European policies, adding cybersecurity aspect to existing regulatory frameworks. (adapted from Analysis of Cyber Security Aspects in the Maritime Sector 2011, p. 24-25)

2.3.2 International Maritime Organization

IMO published the "Guidelines on Maritime Cyber Risk Management" in July 2017 which were approved at IMO's Facilitation Committee's forty-first session in April 2017 and at its Maritime Safety Committee's ninety-eighth session in June 2017. The Guidelines are meant to provide high-level recommendations and functional elements which can be incorporated into existing risk management processes for effective maritime cyber risk management. According to IMO, risk management is fundamental in order to safeguard shipping from current and emerging threats and vulnerabilities caused by "digitization, integration and automation of processes and systems in shipping" – and it is not enough to focus on operations in the physical domain. (Guidelines on Maritime Cyber Risk Management 2017, p. 3)

The Guidelines remind, that while new technologies and ICT systems provide efficiency, at the same time they also add risks to critical systems and processes. The Guidelines define a threat as "presented by malicious actions (e.g. hacking or introduction of malware) or the unintended consequences benign actions (e.g. software maintenance or user permissions)". These actions can expose or exploit a vulnerability in OT or IT which can result from for example imperfect design or integration of systems or shortages in cyber-discipline. The safety and security impacts caused by the exposure or exploitation of vulnerabilities in IT systems must also be considered in effective cyber risk management. (Guidelines on Maritime Cyber Risk Management 2017, p. 4)

According to the Guidelines, rapidly changing technologies make it difficult to address the risk simply through technical standards. Instead, the risk management approach should be resilient and evolving as an extension of already existing safety and security management practices. Multiple control options for cyber risk management, including management, operational, procedural and technical controls, must be considered when weighing potential threats, vulnerabilities and risk mitigation strategies. Effective cyber risk management begins from the management level and the culture of cyber risk awareness needs to get achieved at all levels. This enables holistic, continuous operation and evaluation through effective feedback. (Guidelines on Maritime Cyber Risk Management 2017, p. 4-5)

The Guidelines present a simple goal of maritime cyber risk management: "to support safe and secure shipping, which is operationally resilient to cyber risks". This can be achieved by assessing the organization's current and desired cyber risk postures. Once this is done, gaps can be identified and addressed to achieve the risk management objectives. This requires a prioritized cyber risk management plan. In order to help the organization reach this goal, the Guidelines present five functional elements, noting that the elements are not sequential but continuous and concurrent, supporting effective cyber risk management:

- "**Identify**": definition of personnel roles and responsibilities, identification of potentially ship operation risk-posing systems, assets, data and capabilities
- "**Protect**": implementation of risk control processes and measures, contingency planning against cyber attacks
- "**Detect**": development and implementation of activities to detect cyber events in a timely manner
- "**Respond**": development and implementation of activities and plans for resilience and restoring of systems disordered by cyber events
- "**Recover**": identification of measures to back-up and restore cyber systems affected by cyber events. (Adapted from Guidelines on Maritime Cyber Risk Management 2017, p. 5)

At the end of the Guidelines, several best practices for implementation of cyber risk management are referenced. According to IMO, they are "The Guidelines on Cyber Security Onboard Ships" (2017) by BIMCO, ISO/IEC 27001:2013 (2013) standard and the NIST Framework (2017).

2.3.3 Baltic and International Maritime Council

BIMCO has published "The Guidelines on Cyber Security Onboard Ships" (2017) which are aligned with the Guidelines on Cyber Risk Management (2017) by IMO. BIMCO also mentions that the Framework by NIST was used while developing the Guidelines. According to BIMCO's Guidelines, although the cyber security approaches are company- and ship-specific, they should be guided by "appropriate standards and the requirements of relevant national regulations" (Guidelines on Cyber Security Onboard Ships 2017, p. 5). Another aspect which BIMCO highlights in its Guidelines is that the cyber risk management plans and procedures of the organization should be complementary to the existing safety and security risk management requirements presented in other systems and codes in use, such as the International Management Code for the Safe Operation of Ships and Pollution Prevention (ISM Code), the International Ship and Port Facility Security Code (ISPS Code) and the Safety Management System (SMS).

Figure 3 represents the cyber security approach of BIMCO's Guidelines on Cyber Security Onboard Ships (2017, p. 8). The six core concepts of effective cyber risk management

are identification of threats, identification of vulnerabilities, assessing risk exposure, development of protection and detection measures, establishment of contingency plans and responding to and recovering from cybersecurity incidents. (The Guidelines on Cyber Security Onboard Ships 2017, p. 8)

Figure 3: Cyber security approach of the Guidelines on Cyber Security Onboard Ships (BIMCO 2017, p. 8)

The topics of identification of threats and vulnerabilities were managed in the chapter "1.6.1 Maritime industry specific characteristics and threats" of this thesis. As the first recommendation under the subject of assessing risk exposure, BIMCO's Guidelines suggest the accountability and ownership for the assessment to start from the senior management level of the organization, for multiple reasons including the following:

- Senior management level must evaluate and decide on risk versus trade-offs as their strategic responsibility, since improving cybersecurity may make standard business processes more time consuming or costly.

- Improving cybersecurity may be related to business processes and training rather than to IT systems and for this reason must be handled organizationally.
- Senior management level must decide whether or how to amend relationships with customers, suppliers and authorities, in case improving cybersecurity requires new kind of cooperation between parties.
- When the previous three aspects are clear, it is possible to define the IT requirements of the cyber strategy, which can be done by the IT department.
- The general strategic decisions and risk versus trade-offs guide the development of contingency plans of potential occurring cyber incidents. (Adapted from Guidelines on Cyber Security Onboard Ships 2017, p. 17)

The Guidelines on Cyber Security Onboard Ships (2017) remind to take the range of the characteristics of the maritime industry into consideration while assessing the risk. These characteristics were presented in the chapter "1.6.1 Maritime industry specific characteristics and threats" of this thesis. In the chapter "1.6.4 Confidentiality, integrity and availability model", the CIA model which the Guidelines suggest to be used for the impact assessment, was also introduced. The Guidelines present two approaches for risk assessment - organization's own and third-party assessments. According to the guidelines, the risk assessment process made by the organization should begin by assessing the onboard systems, the goal being mapping their robustness to manage the cyber threats on the current level. The Guidelines suggest to first identify the existing technical and procedural controls protecting IT and OT systems, IT and OT systems that are vulnerable and the specific vulnerabilities, cyber attack vulnerable key ship board operations and the possible cyber incidents and their impact on key ship board operations including the likelihood of their occurrence. The organization can cooperate with the service providers and the producers of the onboard equipment and systems in order to find out about already existing technical controls and procedures related to cybersecurity. (The Guidelines on Cyber Security Onboard Ships 2017, p. 22)

Third-party risk assessments serve as good completions for self-assessments and may help identifying gaps and risks that were not found during the assessment made by the organization. In order to find out whether the organization's defence level matches the one set out in the organization's cyber strategy, penetration tests of IT and OT systems can be made. However, active penetration testing such as social engineering or physical penetration to the facility's security perimeter may only be suitable for IT systems, since OT systems may be so vital that risks related to them cannot be taken. In these cases, passive testing, such as scanning data transmitted by the system, should be considered. The Guidelines introduces a four-phase risk assessment process, which results in a final report including executive summary, technical findings, prioritized list of actions, supplementary data and appendices. Once the findings are handled, it may be necessary to send a subset of findings to the producers of the affected systems and to use some external expert analysis. (The Guidelines on Cyber Security Onboard Ships 2017, p. 24)

The fifth part, developing protection and detection measures, of BIMCO's Guidelines states that the goal and outcome of the cyber strategy should be reduction of risk, if needed. Situations, where it has not been controlled who has had access to the onboard systems, such as drydocking, need special attention. Cyber security protection measures may be technical or procedural, but both technical and procedural controls should be compatible with the CIA model. Only cost effective technical controls should be implemented and the implementation should be prioritized, beginning from those with the greatest benefit. The Guidelines refer to the list of Critical Security Controls (CSC) by The Centre for Internet Security (CIS) and has collected together the most relevant ones to ship onboard equipment and data:

- "limitation to and control of network ports, protocols and services
- configuration of network devices such as firewalls, routers and switches
- physical security
- detection, blocking and alerts
- satellite and radio communication
- wireless access control
- malware detection
- secure configuration for hardware and software
- email and web browser protection
- data recovery capability
- application software security (patch management)
- training and awareness
- access for visitors
- upgrades and software maintenance
- anti-virus and anti-malware tool updates
- remote access
- use of administrator privileges
- physical and removable media controls
- equipment disposal, including data destruction
- obtaining support from ashore and contingency plans" (The Guidelines on Cyber Security Onboard Ships 2017, p. 25-34).

In the last parts of the Guidelines, establishment of contingency plans and responding to and recovering from cybersecurity incidents, it is highlighted that it is important to understand the significance of each cyber incident specifically for IT and OT systems. The CIA model should be used to assess the impact of incidents. Especially loss of OT systems should be taken seriously since it typically immediately affects the safe operation of the ship. The Guidelines remind, that contingency plans for cyber incidents should be addressed by appropriate operational and emergency procedures included in the SMS. Some of the existing procedures in the SMS may also already cover some cyber incidents. The

SMS typically includes "procedures for reporting accidents or hazardous situations and levels of communication and authority for decision making" (The Guidelines on Cyber Security Onboard Ships 2017, p. 35). These procedures can be amended to suit the situations of cyber incidents. The contingency plans should be available in a non-electronic form in case of an incident with data destruction, for example. External expert assistance may be required when handling especially complex or severe incidents.

At the end of the Guidelines, BIMCO suggests information of previous identified cyber incidents to be used when improving the response plan. To achieve an effective response to a cyber incident, a team of "onboard and shore-based personnel and/or external experts" should be built for restoring the IT and OT systems enabling the normal operation of the vessel. The Guidelines present a four-step list for effective response:

- "**Initial assessment**": Answering questions related to how the incident occurred, which systems were affected and how, the extent to which data is affected and to what threats to systems remain
- "**Recover systems and data**": Cleaning, recovery and restoring of IT and OT systems and data in order to return to operational conditions, removing threats and restoring software
- "**Investigate the incident**": Investigation (with external experts) to understand the causes and consequences of the incident – vital role in preventing recurrences
- "**Prevent a re-occurrence**": With the help of the investigation outcome, potential supplement of protection measures. (Adapted from Guidelines on Cyber Security Onboard Ships 2017, p. 37)

According to the Guidelines of BIMCO, the purpose of a recovery plan is "to support the recovery of systems and data necessary to restore IT and OT to an operational state". The focus is on ensuring the safety of the onboard personnel by prioritizing the operation and navigation of the vessel. The recovery plan should be available in hard copy both onboard and ashore and cybersecurity responsible personnel should be able to understand it. In case recovery of OT requires assistance from ashore, it should be clarified in the recovery plan. After recovery, proper investigation of the cyber incident can provide valuable information for both the organization and the maritime industry in a wider context. External expert support may be needed, but the information gained from proper investigation can be used in many helpful ways – for example to improve the technical and procedural protection measures to prevent recurrences, understand potential cyber risks of maritime industry better and identify lessons learned and improve training to raise awareness level. (Guidelines on Cyber Security Onboard Ships 2017, p. 39)

2.3.4 Government of the United Kingdom

The Government of the United Kingdom (UK) published a "Code of Practice – Cyber Security for Ships" (H. Boyes & R. Isbell), referred to as the "Code", in September 2017.

The document is produced by the Institution of Engineering and Technology, supported by the Defence Science and Technological Laboratory and funded by the Department for Transport. After explaining the definition of cybersecurity and the importance of it for vessels, it focuses on providing a management framework with the target of reducing the cyber risk.

The Code's risk management approach to cybersecurity begins with the development of a cyber security assessment (CSA), which acts as a base of the cyber security plan (CSP). On a higher level, the ship security assessment (SSA) and the ship security plan (SSP), which are required by the ISPS code align the development of the CSA and CSP. Based on all these documents, the policies, processes and procedures of the vessel are produced. With the performance of a CSA, the organization is able to assess and mitigate the risks caused by potential threats relevant to vessels and prioritize these risks. This way, appropriate investments to improve the security controls to mitigate the risks with the highest impact can be done. When assessing the risks, four aspects and their relationships must be considered – physical, personnel, processes and technical. (H. Boyes & R. Isbell 2017, p. 21-23)

The Code's CSA process begins with the identification of the important vessel assets such as data, systems and functions, to protect. In the next phase, the vessel's operational processes are identified and their criticality is assessed. It is also required to understand the dependencies between them. In the third phase, the risks arising from potential threats, vulnerabilities and their likelihood of occurrence are assessed. This needs to be done "in order to establish the need for and to prioritise security measures". The fourth phase is the "identification, assessment, selection and prioritisation of security controls and procedural changes". In this phase, their costs and savings and impact on risk reduction and ship operation need to be considered. In the last phase of the CSA process, the acceptability of the overall residual risk is continuously reviewed based on the selected security controls. (H. Boyes & R. Isbell 2017, p. 22)

According to the Code, the CSP which is built based on the CSA and the existing SSP, should establish "appropriate security measures designed to minimize the likelihood of a breach of security and the consequences of a potential risk" (H. Boyes & R. Isbell 2017, p. 23). The completed CSP should be an annex of the SSP and protected from unauthorized access. A holistic approach is mandatory and from the cybersecurity point of view, the CSP should either refer to or contain:

- "the policies that set out the security-related business ruled derived from the SSP;
- the processes that are derived from the security policies and provide guidance on their consistent implementation throughout the lifecycle and use of the ship assets; and

- the procedures that comprise the detailed work instructions relating to repeatable and consistent mechanisms for the implementation and operational delivery of the processes" (H. Boyes & R. Isbell 2017, p. 23).

The Code reminds, that a big part of security breaches is caused by people and poor processes and therefore recommends a careful consideration of personnel, process and physical aspects that relate to technological systems protected with cybersecurity measures. Appropriate measures must be implemented for the previously mentioned aspects as well and they also depend on the targeted cyber resiliency level. The Code highlights the importance of training and assessment of the personnel that have the authority to access the systems of the vessel. (H. Boyes & R. Isbell 2017, p. 23)

The CSP should be at least annually reviewed and based on any identified gaps, "shortcomings or … changes … which impact on the ship or ship assets", updated accordingly. The CSP should also present the monitoring and auditing measures for the full lifecycle of all the assets of the vessel and only "suitably qualified and experienced" actors should complete this work. The Code states, that the monitoring should continue also in the case of failure or interruption of any system. In addition to self-assessment, The Code recommends assessing "the compliance of the vessel's supply chain with the security policies, processes and procedures" of the CSP. Although some responsibility of the compliance can be transferred to a supplier, the company owning the vessel should be accountable of the overall security controls. (H. Boyes & R. Isbell 2017, p. 24-25)

In the last section of the Code, "Managing cyber security", management and operational arrangements are handled. Those arrangements include the identification of the cybersecurity responsible individual(s) of the vessel, "the establishment of a security operations center (SOC)", "the arrangements for providing information to third parties" and "the arrangements for managing security incidents or breaches". The Code recommends a designation of a cyber security officer, CySO, which should be in charge of all security aspects of cyber systems on the vessel and aware of legal and regulatory changes that could potentially affect the vessel's policies, processes and procedures. Additionally, the CySO should cooperate with the Company security officer (CSO), ensure "the development, periodic review and maintenance of the CSA/CSP" and be responsible for the implementation and exercising of the previously mentioned. Cybersecurity specialists' advice may be used when CySO's knowledge of the topic and appropriate solutions is imperfect. CySO's cybersecurity responsibility may also be shared "with other managers and service providers", but the CySO remains accountable. (H. Boyes & R. Isbell 2017, p. 27-28)

Finally, the Code recommends establishing a security operations center (SOC). A SOC is a central unit handling security issues related to the cyber-physical systems of the vessel. In case of a cybersecurity related event or unfolding circumstances, the main functions of a SOC are to observe any type of threats to the vessel, orient through risk analysis

"whether proactive measures are required to reduce the risk to an acceptable level", decide the appropriate actions and act by implementing these decisions. A SOC personnel may need to access "threat intelligence information from both public and private sector sources" in order to better be aware of the general threat environment. As an example of this kind of threat intelligence sharing scheme the Code mentions the Cyber Security Information Sharing Partnership (CiSP), which is a joint industry and government initiative launched in 2013 and operated by the National Cyber Security Center of the United Kingdom. The Code lists several benefits of participating in an information sharing scheme like this – for example early warning of cyber threats and the chance to learn from experiences of other users and seek help. (H. Boyes & R. Isbell 2017, p. 29-30)

2.4 Classification societies

In this chapter, the cybersecurity approaches of selected classification societies are introduced. The publications of this chapter are released by Lloyd's Register, DNV GL and American Bureau of Shipping.

2.4.1 Lloyd's Register

Lloyd's Register's approach "Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping" (2016) to assuring the safety and security of today's cyber-enabled vessel begins with the definition of a cyber system and the term cyber-enabled, which were handled in the chapter "1.6.2 Information and operational technology systems" of this thesis. The publication, referred to as the "Guidance Note", lists six key areas of risk to be considered and addressed when assuring the safety and dependability of a cyber-enabled vessel: system, human-system, software, network and communications, data assurance and cybersecurity. LR recommends a risk-based assurance process and references ISO/IEC standards as well as its own LR Rules for governance and guidance of ICT requirements. The Guidance Note is followed by the "Cyber-enabled Ships - ShipRight Procedures - Autonomous Ships – Guidance Document" (2016) which should be read in conjunction with the Guidance Note. The ShipRight Procedures dig deeper and provide tools for addressing the requirements for detailed system design. (Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping 2016, p. 1; ShipRight Procedures – Autonomous Ships 2016, p. 1)

According to LR's Guidance Note, the assurance of the cyber-enabled vessel begins by the identification of safety critical systems and ensuring their resiliency and graceful degradation in case of failure. In order to do this, "the fault tolerance and the defence control and monitoring functions needed for the services and systems critical to safety or the business need to be identified" (Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping 2016, p. 4). A risk-based approach, such as LR's own "Assessment of Risk Based Design" (ARBD) process or for example the NIST

Framework can be used. The Guidance Note also reminds, that the remote connection to systems on shore create an extra level of complexity and risk and additional questions, such as "are the onshore systems maintained, patched and protected to an acceptable standard?" must be answered when assessing the risk.

LR's Guidance Note states, that the assisting or replacing of seafarers or tasks that operate the vessel which ICT enables potentially offers benefits, but in order to achieve this the vessel's design must address the human-system issues emerging from the use of ICT. A successful design considers the changed expectations targeted to the users for operation and failure diagnose of the systems, re-design of the work of seafarers and off-shore staff, the impact of changes on safe and efficient performance of the staff and the need to monitor ship operations. The Guidance Note suggests a structured, human-based approach to be used and references the ISO 9241-210 Human-Centred Design (HCD) for Interactive Systems standard (2010). (Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping 2016, p. 7)

When considering networks and communications, LR's Guidance Note notes, that the suppliers are expected to provide safe and secure systems, but often these systems have not been tested as part of the complete system in the environment they are intended to be used. For this reason, it needs to be ensured that the network components are of correct maritime environment standard and enough spares for critical infrastructures are available on board, the communications bearer and maintenance are functional especially if systems are supported from on shore, the internal networks offer sufficient data capacity, the safety and business critical systems can be prioritized by the staff when necessary and the data transfer is fast enough to operate the ship safely and securely without compromising data integrity. (Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping 2016, p. 8)

LR's Guidance Note highlights the increasing importance of software (SW) maintenance because of the high level of SW integration and reliance on correctly operating SW. The production and maintenance should fill the requirements of a recognized international or national standard, such as IEC 61508:2010 (2010) "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems". According to the Guidance Note, a good engineering process considers the complexity of SW including its failure mechanisms and general third-party provided components, as well as defines the documentation needed for producing the SW, communicating the "requirements, design, operation, constraints, limitations and maintenance to the software product's stakeholders". (Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping 2016, p. 8)

In LR's risk-based approach to SW assurance, the goal is to manage the general risk caused by the characteristics of the SW and the specific risks related to a certain SW application. LR's "Provisional Rules and Regulations for Software to be used in Naval

Ships" (2016) are referenced to offer detailed guidance related to the topic. According to the Guidance Note, it is the producer's responsibility to "demonstrate that the practices it uses are suitable and adequate" and the degree of oversight of the production of SW is evaluated based on specific criteria, for example the maturity of the producing organization. Additionally, the SW production must be delivered in accordance with the ISO 9001:2015 (2015) standard for quality management. What it comes to SW maintenance, the Guidance Note brings up the importance of proper SW configuration management, since due to the high level of integration of systems, any changes made to individual systems may raise the risk of failure of the overall system. Again, ISO 9001 and ISO 10007:2017 (2017) standard for configuration management are referenced to help with the implementation of suitable SW configuration processes. (Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping 2016, p. 9)

In the end of the Guidance Note, LR points out that although data is extremely vital to any organization, at lot of organizations are not able to handle their data effectively – they might not know what data they hold, what they need or the quality of the data. The organizations need to follow a criteria for data assurance at the system design: "integrity, availability, authentication, confidentiality, authorization, non-repudiation" and safety-preserving data properties. The Guidance Note also highlights the need to secure critical maritime systems from the increased cyber threats, especially because the global economy is increasingly dependent on maritime trade. According to LR, cybersecurity is a "through-life issue" beginning from project inception to asset disposal, referring to ISO/IEC 27001:2013 (2013) and ISO/IEC 15408 (2008 & 2009) standards. The role of education and related organizational culture is significant when considering cybersecurity. Finally, LR states that connectivity is the element making the marine environment unique for cyber incidents. Also, the fact that vessels often have 64 Kb Inmarsat connection between systems rather than a 50 or over Mb broadband causes the fact that any files needed for recovery in the event of cyber attack need to be located onboard instead of being downloaded, since downloading would take an unbearably long time. Nevertheless, most vessels do not have for example operating system disks onboard which serves as a single point of failure and vulnerability. (Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping 2016, p. 10-11)

2.4.2 DNV GL

DNV GL's "Recommended Practice – Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation" (2016), referred to as the "Recommended Practice", begins with quotations from the ISM Code and IMO Guidelines on Maritime Cyber Risk Management (2017). In addition to these publications, the Recommended Practice is built on BIMCO's Guidelines on Cyber Security Onboard Ships (2017). In the beginning of the Recommended Practice, DNV GL presents the categorization of threats with

examples. These were introduced in the chapter 1.6.1 “Maritime industry specific characteristics and threats”. After this, the Recommended Practice lists three factors for improving cybersecurity:

- “assessment”
- “improvement”
- “verification and validation” (Recommended Practice – Cyber Security Resilience Management 2016, p. 8).

According to DNV GL’s Recommended Practice, there are multiple common aspects in cybersecurity resilience with quality management systems. The Plan-Do-Check-Act (PDCA) cycle, concept of continuous improvement of processes and compliance with the ISM and ISPS Codes are relevant. In the beginning of the document, DNV GL also mentions ISO/IEC 27001:2013 (2013) and IEC 62443-3-3:2013 (2013) as requirement placing standards. (Recommended Practice – Cyber Security Resilience Management 2016, p. 8)

DNV GL’s Recommended Practice recommends three different approaches for assessment – high level, focused and comprehensive, in-depth assessment. The high-level assessment is categorized as senior management’s responsibility while focused assessment is done for specific systems and data sets and comprehensive assessment for generation of a comprehensive image of the total cybersecurity risk of the organization. The four steps of the high-level assessment are:

- identification of key systems of the company
- consideration of the consequences of a cyber attack (with the help of the CIA model and impact assessment presented in the chapter 1.6.2 “Confidentiality, integrity and availability model” of this thesis)
- assessing the likelihood of a cyber attack
- displaying the results of the previous two steps in a risk matrix. (Adapted from Recommended Practice – Cyber Security Resilience Management 2016, p. 14)

After the high-level assessment, the organization has an overview of its cybersecurity risk picture and with the help of these results, it can begin focusing on where more detailed assessment is needed. Focused assessment is recommended for systems and datasets which “are placed in the unacceptable part of the risk matrix”. The four steps of the focused assessment are:

- identification of threats to systems, that support specific vessel functions and business processes
- identification of barriers preventing incidents related to these threats
- identification of barriers reducing the consequences, in case these incidents occur

- assessing the robustness of these preventive and consequence reduction barriers. (Adapted from Recommended Practice – Cyber Security Resilience Management 2016, p. 15)

Barrier in cybersecurity can be an "action, device, procedure, or technique that reduces the threat, vulnerability or an attack by eliminating it, or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective actions can be taken". DNV GL suggests the Bow-Tie method to be used during focused assessment. The Bow-Tie method helps the quick visualization of whether more cybersecurity measures should be implemented, since it does not focus on the probability or frequency of the attack – instead it assesses the risks, controls and barriers against certain attack. Bow-Tie diagrams are also an effective way to build awareness of cybersecurity efforts and with them, the Core Functions defined in the NIST Framework can be found. The main components of the Bow-Tie method are "hazard, top event, threats, consequences and barriers". The Recommended Practice provides various lists of questions, actions and categorizations to help the identification of necessary components to complete the focused assessment. (Recommended Practice – Cyber Security Resilience Management 2016, p. 18-21)

The comprehensive, in depth assessment is more technical and may require external expert assistance to be completed. It is used when a more detailed assessment is needed and is related to the critical business processes. The five steps of the comprehensive, in depth assessment are

- identification of the critical IT/OT systems (by mapping them to business processes)
- identification of the consequences of a cyber attack for each system (with the help of the CIA model and impact assessment presented in the chapter 1.6.2 "Confidentiality, integrity and availability model" of this thesis)
- determination of the ease of access to each of these systems
- rating of the systems regarding their cybersecurity risk (likelihood X the consequences of the attack)
- comparison of current safeguards with the target level. (Adapted from Recommended Practice – Cyber Security Resilience Management 2016, p. 21)

The Recommended Practice provides various lists of questions, actions and categorizations to help identification of necessary components to complete the comprehensive, in depth assessment as well as the focused assessment. After briefing the use of CIA model, the Recommended Practice gives an example of the determination of the likelihood of an attack and the construction of a risk matrix. When combining the results of these actions, the systems can be rated regarding their cybersecurity risk and comparing of current safeguards with target can be done. For IT systems, the Recommended Practice and its Appendix E provide practical guidance on how to build "more detailed checklists referencing

the technical prioritized verifiable control points" based on the requirements of the "BSI Grundschutz catalogue" (2013), which is aligned with ISO/IEC 27001 (2013). For OT systems, the Recommended Practice and its Appendix F provide guidance on how to build checklists based on the requirements of IEC 6443-3-3 (2013). (Adapted from Recommended Practice – Cyber Security Resilience Management 2016, p. 22-28)

The assessments introduced in the previous sections help the organization find its areas of improvement. In the "improvement" section of DNV GL's Recommended Practice, mitigation options for risks are first introduced. These responses were presented in the chapter 1.6 "Definition of cybersecurity in maritime industry" of this thesis. The Recommended Practice states, that a cost benefit analysis is mandatory when defining the most efficient risk mitigation strategy. This requires viewing the cybersecurity risk picture of the organization – it can be used to build financial models to support investment decision making for improvement actions. Previously presented Bow-Tie method and cyber risk matrix are proposed to be used as tools. When reducing the risk is desired, respective checklists and a work plan based on these is proposed. Because the risk picture constantly changes, it is required to use continuous improvement cycles, such as the PDCA to ensure that the checklists and procedures remain up to date. Through continuous improvement, the organization's cybersecurity maturity and resilience level can grow from reactive to predictive and finally, proactive. (Recommended Practice – Cyber Security Resilience Management 2016, p. 29-30)

DNV GL's Recommended Practice states, that the improvements can concern general awareness and training, be of more technical nature or relate to creating an ISMS. The Recommended Practice highlights the meaning of the human factor in cybersecurity – for example social engineering and phishing are common. Insider threat must also be considered. It is very important to build awareness and competence, since staff in many organizations is unable to react correctly in case of a cybersecurity incident. "The desired behaviour and awareness … needs to be evaluated just like any other objective". As technical improvements in the maritime and offshore industries, the Recommended Practice mentions for example network segregation and hardening secure remote connections. The Recommended Practice also states that it may be valuable for the organization to establish an ISMS based on the IEC/ISO 27001 (2013) standard, which can be integrated to the organization's integrated management system. While the Recommended Practice focuses on the operational aspects of cybersecurity management, IEC/ISO 27001 standard complements it with organizational point of view. The Recommended Practice provides a list of Clauses of IEC/ISO 27001 which it covers, which it does not cover and guidance on how to achieve full cover of the standard and an effective ISMS. (Recommended Practice – Cyber Security Resilience Management 2016, p. 31-35)

The final section of DNV GL's Recommended Practice presents approaches for validation and verification after the assessment and improvement actions have been completed. First, monitoring and testing of technical barriers is introduced. This can be divided to

testing of components and testing of systems. In both cases, testing on a recurring basis is recommended. For component level testing, the guidance of IEC 62443-4-2 (2017) and IEC 61162-460:2015 (2015) standards is referred to. After component level testing, the system can be tested in different ways – by actively provoking failures or periodically repeated passive measurements and by penetration tests. The topics were also presented in the chapter 2.3.3 "Baltic and International Maritime Council" of this thesis. When testing, "verification by an accredited third party can add value", especially when validating the ISMS as a whole. The certification received from the worldwide recognized third party may also drive the continuous improvement cycle of cybersecurity. (Recommended Practice – Cyber Security Resilience Management 2016, p. 36-38)

2.4.3 American Bureau of Shipping

American Bureau of Shipping (ABS) released the industry's first risk-based management program, ABS "CyberSafety™" series, which presents best practices for safety and security of four key cyber areas of marine and offshore environments: "cybersecurity, automated systems safety, data management and software assurance" (Cybersecurity – Guidance Notes for the Marine and Offshore Industries 2016, p. 2). The program is described as "measurable implementation of CyberSafety that tailors cybersecurity and systematic safety to assets in order to enable and encourage risk-based asset management as a systematic outcome" (J. Jorgensen 2016, p. 9). The program consists of a family of five documents:

- "Volume 1: Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations" (referred to as "Volume 1")
- "Volume 2: Guide for Cybersecurity Implementation for the Marine and Offshore Industries" (referred to as "Volume 2")
- "Volume 3: Guidance Notes on Data Integrity for Marine and Offshore Operations"
- "Volume 4: Guide for Software Systems Verification"
- "Volume 5: Guidance Notes on Software Provider Conformity Program".

This thesis focuses on introducing the first two volumes of the series to give the reader a good overview of the program, since the three last documents of the series concentrate on providing detailed technical direction for the implementation of thorough cybersecurity.

Volume 1 of ABS CyberSafety™ series first explains how growing software and automation dependence and integration of systems of the maritime industry makes proper cybersecurity and software integrity management increasingly important in order to widely understand the linked systems, software and overall system safety. The CyberSafety™ program answers these needs by presenting a Capability model which helps the organization add cybersecurity to its OT systems and to the linked business systems. A Capability has a wide definition, since it includes "people, systems, data and processes".

The idea of the program is to gradually build these capabilities "based on security needs, staff competencies, available acquisition resources and organizational maturity in cybersecurity". (CyberSafety™ – Volume 1 2016, p. 10)

The Capability model of ABS CyberSafety™ Volume 1 presents three sets of capabilities: Basic Capabilities, Developed Capabilities and Integrated Capabilities – a total of 37 capabilities, which serve as the primary elements of the organization's cybersecurity program and their implementation can be prioritized in a measurable way. Appendix A presents the full capability model, in which the first nine capabilities form the Basic Capability Set, capabilities from ten to 23 present the Developed Capability Set and the final capabilities from 24 to 37 build the Integrated Capability Set.

In the next parts of the ABS CyberSafety™ Volume 1 document, Best Practices for each of the Capability are introduced. The Best Practices are constructed based on multiple sources, including different industries, government reports and white papers. For each Capability Best Practices, a list of references is provided for further understanding. For example, one of the Best Practices for the first capability of the Basic Capability Set, "Exercise Best Practices", is presented as follows: "The organization uses regional and national resources (e.g., US-CERT, ICS-CERT and ENISA) to gain access to recent vulnerability and threat information relevant to its assets" (CyberSafety™ – Volume 1 2016, p. 15). In the end of the chapter, the reference list includes links to relevant references, including all the mentioned organizations that were mentioned in the Best Practice.

The Volume 2 of the ABS CyberSafety™ program follows the Volume 1 by providing implementation specifications for the capabilities and linking systems engineering and cybersecurity. The goal is to build a Capability-Task-Assessment cycle and develop a risk profile for the assets and collections of assets. Volume 2 "provides criteria for the assessment of corporate systems and asset readiness to prevent cyber events that my compromise the safety and security of the data, systems and assets". In the Volume 2, an optional "CS" series (CS1, CS2 and CS3) Class Notation is offered. It may help the organization to indicate its preparedness for cybersecurity concerns. The categorization is based on the requirements presented in the document and is suitable for all vessels compliant with the ISM Code. An organization compliant with the procedures and criteria defined in Volume 2 may receive a CyberSafety Management System Certificate (CMSC) and Notation CS1, CS2 or CS3 (in case of an ABS classed vessel, otherwise a "Statement of Fact") or a Certificate of Cyber Compliance (CCC) for an examined facility. (J. Jorgensen 2016, p. 11; CyberSafety™ – Volume 2 2016, p. 2-7)

Figure 4 presents the Notation hierarchy of ABS CyberSafety™ Volume 2. The levels of Notation build on the implemented Capabilities. This means, that increasing the capability implementation is the way for the organization to move up to the higher Notation level. The CS Notation level also describes the organization's level of cybersecurity maturity.

The CS Notation levels are linked to the respective sets of Capabilities presented in Volume 1 of the program. When implementing the Basic Capability Set, the organization can reach the CS1 level, by the Developed Capability set the CS2 level can be reached and by the Integrated Capability Set, the highest C3 level can be achieved. (CyberSafety™ – Volume 2 2016, p. 22)

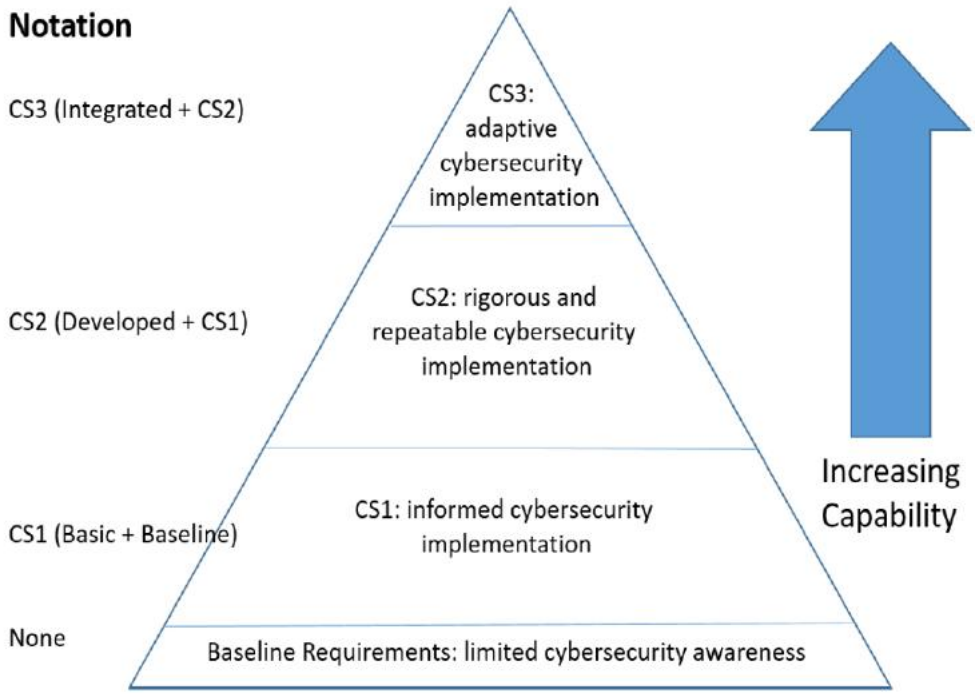


Figure 4: ABS CyberSafety™ - Notation hierarchy (CyberSafety™ – Volume 2 2016, p. 22)

Following the explanation of the Notation hierarchy, Volume 2 provides a more detailed description of the requirements of each level, as well as an overview of the capability assessment process. The main focus of the document is in the Capability Matrix, which establishes the Best Practices and defines and provides "the organizational process specification for each capability together with the associated IT and OT specifications" (CyberSafety™ – Volume 2 2016, p. 30). Appendix B presents an example of how the first capability, "Exercise best practices", of the Basic Capability Set is displayed in the Capability Matrix and the specifications and requirements related to this capability.

At the end of Volume 2, it is stated that if the organization desires to achieve the ABS CyberSafety™ certification, it needs to establish a Cybersecurity Management System (CMS) in order "to implement and monitor its security strategy and plan". The CMS is the framework for capability and tracking management as well as the key for the organization to grow its capabilities to desired levels, to support "operational understanding of security posture(s); satisfying audit requirements; and provisioning and maintaining security continuous monitoring (SCM) needs" (CyberSafety™ - Volume 2 2016, p. 104). Volume 2 presents a list of requirements set for the CMS to be able to demonstrate, plan,

implement and operate such system. In the last chapter of the document, requirements for the maintenance of the classification with the ABS CyberSafety™ Notation are presented. (CyberSafety™ - Volume 2 2016, p. 114)

2.5 Potential future influencers

In this chapter, publications that may have future influence on the actions of ABB are processed. The material of this chapter is produced by Bureau Veritas and United States Coast Guard.

2.5.1 Bureau Veritas

In 2016, Bureau Veritas (BV) published "Cybersecurity of Connected Vehicles Guidelines", from now on referred to as the "Guidelines". The Guidelines present a set of cybersecurity objectives and best practices for manufacturers and supplies for securing their vehicles against cyber threats, concentrating on the automotive industry. However, the publication was found interesting for the research of this marine industry focused thesis since the appearance of autonomous vessels is in the near future for this industry as well. (Cybersecurity of Connected Vehicles 2016, p. 6)

In the beginning of the Guidelines, BV brings up the fact that the embedding of new features which are exposed to cyber attacks may affect the vehicles confidentiality, integrity and availability properties. In case of a successful cyber attack, the vehicle's internal data may get intercepted, the vehicle fleet can be immobilized or the vehicle may become controlled, modified or even stolen remotely by the attacker. BV mentions that the lack of common public cybersecurity standard for vehicles prevents manufacturers and suppliers from sharing references and this is why each of them has created their own strategy. This causes lack of knowledge transfer and interoperability "when attackers are becoming more organized and attack methods (and modes) are evolving very fast" (Cybersecurity of Connected Vehicles 2016, p. 6).

BV's Guidelines list some existing cybersecurity standards and frameworks, including the IEC 62443 (2016) series of standards and NIST Cyber Framework (2017), but explain that those are generic and do not take into account the "specificities of vehicles". The Guidelines aim to consider these specificities and provide best practices for addressing cybersecurity risks. The Guidelines are based on two widely used reputable norms, ISO 27001 (2013) Information Security Management standard and ISO 26262 (2011) standard for functional safety to the automotive industry. (Cybersecurity of Connected Vehicles 2016, p. 7)

The Guidelines of BV consist of three main parts: Security Governance, Development Cycle Objectives and Operation and Maintenance Objectives. The first part begins with the Security Level Identification and concentrates on managing the cyber risk during the

whole lifecycle of the vehicle. The second part specifies objectives for the design phase of the vehicle considering the system, hardware and software aspects. The last part focuses on the specification of objectives for a released vehicle, including the Update Management, Cyber Security Intelligence and Remediation Measures. The objectives presented in each part are spread in three Security Levels (SL) defined in the first part of the Guidelines and reflecting the gradually increasing implementation level of the security management process. When defining the target Security Level, the organization needs to consider the level of automation and connectivity of the vehicle, "the legal or financial consequences of a security breach" and the "impact on the safety of individuals". (Cybersecurity of Connected Vehicles 2016, p. 8-14)

As an example, the first objective presented in the first part of the Guidelines of BV, considers "Security criteria". It is targeted to the manufacturers and begins with a reference to the CIA model – "The Availability, Confidentiality and/or Integrity criteria shall be selected and defined for each relevant asset or resource that the vehicle may expose directly or indirectly to cyber attacks". The first objective also provides a list of example assets, such as the driving subsystem, navigation system history or current destination and the driver's contact list. The objective proposes that this list of assets "shall be representative of all the business, safety of privacy impacts that a failure of the embedded systems may have". In a similar style, the Guidelines present a list of objectives for each main part and each Security Level. The comprehensive implementation of the objectives enables the reduction of cyber security risks, which BV identifies as one of the main goals for the manufacturers. (Cybersecurity of Connected Vehicles 2016, p. 14)

2.5.2 Unites States Coast Guard

In 2015, United States Coast Guard (USCG) published their "Cyber Strategy" which recognizes cybersecurity as one of the major economic and national security challenges the United States is facing as a Nation. The growing amount of cyber threats poses risk not only to the Maritime Transport System (MTS) and critical infrastructure, but furthermore to the Nation's security and economic stability. The first response to meet the growing cybersecurity requirements is to adapt strategically and to recognize cyberspace as an operational domain. USCG sets out three strategic priorities for the effective operation on the cyber domain – "defending cyberspace", "enabling operations" and "protecting infrastructure". These priorities are presented in the publication with respective more specific goals and objectives. (Cyber Strategy 2015, p. 9)

In order to ensure long-term success, meeting the strategic goals on the cyber domain and to support the previously mentioned three strategic priorities, USCG presents seven supporting factors:

- "recognition of cyberspace as an operational domain,
- developing cyber guidance and defining mission space,

- leveraging partnerships to build knowledge, resource capability, and an understanding of MTS cyber vulnerabilities,
- sharing of real-time information,
- organizing for success,
- building a well-trained cyber workforce and
- making thoughtful future cyber investments" (Cyber Strategy 2015, p. 12).

Following the Cyber Strategy, in 2017 USCG and the Department of Homeland Security (DHS) published a draft version of the "Guidelines for Addressing Cyber Risks at Maritime Transportation Security ACT (MTSA) Regulated Facilities", from now on referred to as the "Guidelines". The Guidelines were open for public commenting until the 11th of September, 2017 and consist of two parts. The first part, Enclosure 1, focuses on presenting existing regulatory requirements in Title 33 of the Code of Federal Regulations (CFR), subchapter H, Maritime Security and how they relate to cybersecurity. The second part, Enclosure 2, concentrates on guiding how to create an enterprise-wide cyber risk management governance program based on the NIST Framework and NIST Special Publication 800-82 (K. Stouffer et al. 2015) on Industrial Control Systems (ICS) Security. Details and specific examples of the development and implementation of a Cyber Risk Management Program (CRMP) are provided. (Guidelines for Addressing Cyber Risks 2017, p. 1)

Enclosure 2 of the Guidelines of USCG widely exploits the concepts of the NIST Framework and significant weight is put on the third subchapter of it, "Consequence Analysis, Vulnerability Analysis, and Mitigation Prioritization". The Guidelines provide five tables for cyber risk evaluation:

- **Table 1**: For the evaluation of consequences, classification of events in five categories varying between "insignificant" and "catastrophic" is provided. A score from 1 to 5 for an event is assigned. The table helps the identification of systems for which further analysis is necessary.
- **Table 2**: Based on the score of event from the previous table, recommended assessment actions are provided. The table helps the prioritization of systems "for which a disruption would have the most severe consequences".
- **Table 3**: For the "Connective Vector Assessment", a set of "YES" or "NO" questions is presented. The table helps the determination of "which systems perform or relate to … critical security and safety functions".
- **Table 4**: For the "Cyber Infrastructure Vulnerability Assessment", a set of "YES" or "NO" questions is presented. Systems with a consequence score of 3 or higher from the first table and systems with a "YES" answers from the previous table should be evaluated.
- **Table 5**: For the "Vulnerability Severity Assessment", a questionnaire is presented. The key is to define the systems with "both an infrastructure vulnerability

> and a vector by which it could be exploited". The questionnaire is answered for each system with a "NO" answer from the previous table. The systems with the highest total score are considered the most vulnerable. (Guidelines for Addressing Cyber Risks 2017, p. 17-19)

B. Segalis and A. Rudawski point out the emphasis of the USCG Guidelines on Connective Vector Assessments which are used for the evaluation of connections between systems and "how these connections may impact or disrupt networks and connected systems" (B. Segalis & A. Rudawski 2017). Segalis and Rudawski mention the example in the Guidelines, according to which regulated facilities are expected to evaluate the possible effect of low risk systems on critical systems – they "may access and compromise critical systems in the event of a cyberattack". (B. Segalis & A. Rudawski 2017)

2.6 Summary of the literature and industrial practices review

The literature and industrial practices review demonstrated, that different actors of the maritime sector are currently releasing their own approaches and best practices on cybersecurity and new publications appear frequently. The industry has recognized the need of developing common cybersecurity standardization. A risk-based approach acts as a predominant point of view, regardless of the publisher. New cybersecurity guidance follows commonly recognized international standards such as ISO/IEC 27000 (2016) family of standards and IEC 15408 (2008 & 2009) for IT security by ISO and IEC. IEC 62443 (2016) standard for IACS security and IEC 61508 (2010) functional safety standard for electrical/electronic/programmable electronic safety-related systems provide guidance for the OT safety and security. Commercial or partly commercial frameworks for holistic enterprise IT management, such as the COBIT 5 (2012) and the ISF Standard of Good Practice for Information Security 2016, which covers ISO/IEC 27002:2013, COBIT 5 and the NIST Framework (2017), have been published.

The NIST Framework appeared as an influential benchmark for cybersecurity assessment. Presenting a risk-based approach, this flexible and technology-neutral framework complements the risk management process and cybersecurity program of the organization. The NIST Framework is based on identifying the current and target cybersecurity states and continuously identifying and prioritizing the cybersecurity improvement opportunities. The Framework also provides a comprehensive list of industry accepted standards to guide the implementation of improvements and offers a chance to communicate cybersecurity with important stakeholders.

ENISA's analysis (2011) pointed out the ICT robustness against cyber attacks, fragmentation of the sector to different levels and low cybersecurity awareness as key challenges of the maritime sector. ENISA's recommendations of implementing awareness raising campaigns and developing a common strategy and best practices by adding the cybersecurity aspect to the physical safety and security policies of the maritime industry predicted

the common trend – the holistic risk-based approach with proactive cyber and information security risk management practices. ENISA highlighted the importance of information sharing between different actors and the harmonization and aligning of policies. IMO's Guidelines on Maritime Cyber Risk Management (2017), which adapt the NIST Framework with the current and target cybersecurity profiles, can be thought of as a response to ENISA's analysis. IMO's Guidelines introduced five functional elements for effective and continuous cyber risk management: Identify – Protect – Detect – Respond – Recover. Further on and aligned with IMO's Guidelines and the NIST Framework, BIMCO published more comprehensive and detailed Guidelines on Cyber Security Onboard Ships (2017). In the heart of BIMCO's approach, there are six core concepts of effective cyber risk management: identification of threats and vulnerabilities, assessing risk exposure, developing protection and detection measures, establishing contingency plans and responding to and recovering from cybersecurity incident.

Code of Practice – Cyber Security for Ships (H. Boyes & R. Isbell 2017) published by the Government of the UK was explored as an example of a state-level response to the topic of maritime cybersecurity. The Code provides a comprehensive information package beginning from the definition of cybersecurity, to the management framework for reducing the cyber risk. The Code also represents a risk-based approach through its concepts of cyber security assessment and cyber security plan based on the ship security assessment and ship security plan, but differently from previously presented publications, does not refer to the NIST Framework at any point. The Code, however, provides a description of cybersecurity responsible individuals and recommends organizations to establish a security operations center as well as to belong to a cybersecurity information sharing scheme such as CiSP.

Classification societies are complementing their rules by publishing recommended practice guidance. LR's approach for a cyber-enabled vessel's safety and security assurance (Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping 2016) identifies six key areas of risk: system, human-system, software, network and communications, data assurance and cybersecurity. LR recommends a risk-based approach such as the NIST Framework or LR's own ARBD process to be used, as well as a structured human-based approach ISO 9241-210 (2010). This eases the consideration of human-system issues arising from the use of ICT instead of seafarers. LR's approach also highlights the increasing importance of SW maintenance because of the SW integration and complete network and communication safety and security when the overall system consists of multiple systems. To implement this, good engineering processes and compliance with IEC 61508 (2010) are needed. LR describes cybersecurity as a through life-issue requiring effective education and strong organizational culture, without forgetting the industry specific factors such as Inmarsat connections and remote connectivity making the marine environment unique for cyber incidents.

DNV GL's Recommended Practice (2016) makes a reference to IMO's and BIMCO's guidelines as well as to the NIST Framework and introduces three factors for improving cybersecurity: assessment, improvement, verification and validation. According to DNV GL, coordination to quality management can be done and for example the PDCA cycle is mentioned. DNV GL divides their approach to high-level, focused and comprehensive, in-depth assessment which can be used for different purposes. DNV GL's approach aims at rating of assets regarding their cybersecurity risk and comparing current and target safeguards and uses tools such as risk matrices, bow-tie method and CIA model in order to achieve this. The importance of cost benefit analysis is noted when choosing improvement opportunities. Focus is also given to the importance of the human factor – "desired behaviour and awareness … needs to be evaluated just like any other objective". For the verification and validation, proper system and component testing is encouraged, as well as third party testing and certification to add value.

ABS has launched the industry's first cyber risk management program, CyberSafety™ series (2016). The four key cyber areas identified by ABS are cybersecurity, automated systems safety, data management and SW assurance. The offering of ABS's program is the Capability model, which consists of the Basic, Developed and Integrated Capability sets. These 37 capabilities are primary, measurable elements for the implementation of a cybersecurity program. The program links system engineering and cybersecurity and offers a CS Class Notation and requirements to reach each Class level, connected to the different Capability sets and a list of reference standards. The higher implementation of the capabilities, the higher CS Notation level can be achieved. An organization complying with the requirements may receive certification with Notation (CS1, CS2 or CS3) for the examined facility. The certification indicates the organization's level of preparedness for cybersecurity concerns and its cybersecurity maturity.

BV's Cybersecurity of Connected Vehicles Guidelines (2016) is produced for the actors of the automotive industry, but was inspected to compare the best practices of the maritime and automotive industries. BV offers a similar approach with reference to the NIST Framework and common, previously listed IEC standards, highlighting the embedding of new features exposed to cyber attacks and the lack of common public cybersecurity standardization for vehicles as key challenges. BV's guidelines divide the lifecycle long cyber risk management to three parts: Security Governance, Development Cycle Objectives and Operation and Maintenance Objectives. The guidelines also offer a Security Level categorization for objectives presented in each part, describing the cybersecurity maturity level similarly to ABS's approach.

USCG's Cyber Strategy (2015) focuses on adapting strategically and recognizing cyber space as an operational domain, with three priorities: "defending cyber space", "enabling operations" and "protecting infrastructure". Following the Cyber Strategy, USCG published Guidelines for Addressing Cyber Risks at Maritime Transportation Security ACT

(MTSA) Regulated Facilities (2017) together with the DHS. This publication offers guidance on creating and enterprise-wide cyber risk management governance program based on the NIST Framework and NIST SP 800-82 (K. Stouffer et al 2015). The guidelines put emphasis on consequence and vulnerability analysis and mitigation prioritization and offers tables with sets of questions and a rating method to complete this. The guidelines additionally put weight on the evaluation of the connections between systems to revel the possible effects of low risk systems to critical systems.

3. AN APPROACH TO UNIFIED CYBERSECURITY PROCESS

This section represents the empirical and practical areas of the research. In this section, the research questions raised in the first part of this thesis are answered. The goal is to improve and unify the cybersecurity project execution process and procedures of ABB Marine. In order to achieve this, it was mandatory to investigate the current state of the cybersecurity project execution process in different locations to find out any best practices to share without an excessive demand of resources within various local business units. Discussions with multiple experts were organized for the validation of the findings. First, methodology for the process unification is provided for other companies to reptile and adapt, followed by the description of the cybersecurity workshops the writer attended and the analysis of customer needs and expectations. After this, the improvement areas and suggestions for improvement for ABB Marine's cybersecurity requirements and project execution process are identified based on the previous literature and industrial practices review section and the outcome of the workshops. Finally, based on the previous steps, the key areas of focus for the unification of ABB Marine's cybersecurity project execution process are presented. The work presented in this section was completed from the perspective of a project.

3.1 Methodology for the unified process

The key for implementing a global cybersecurity project execution process unification is information gathering, analyzing and sharing between different local business units. Since the current cybersecurity project execution process of ABB Marine varies between different local business units and in some areas, may be undefined, it adds challenge to the task. In this thesis, the state of the current cybersecurity project execution process and best practices of different locations were investigated through workshops. The used agenda for the workshops can be defined by the implementing actor in question depending on what the topic and goal of the investigation is. The original agenda used for the workshops in this thesis can be found in the following chapter "3.2 Workshops".

Figure 5 models the process aiming at the global unification of the cybersecurity project execution process of this thesis and is now described. Since the unification process is extensive, it cannot be completed by a sequence of actions but requires a process of continuous improvement and prioritization of items. The unification begins from a global level decision by the cybersecurity organization of the company – the need for global process unification needs to be identified. After this, the company needs to decide which local business unit (LBU) is in charge of the implementation of the unification, in this case ABB Marine Finland (LBU FI). Further decisions of the use of resources is required

when finding the person(s) to complete the task. In this example, a master's thesis worker was hired to the position.

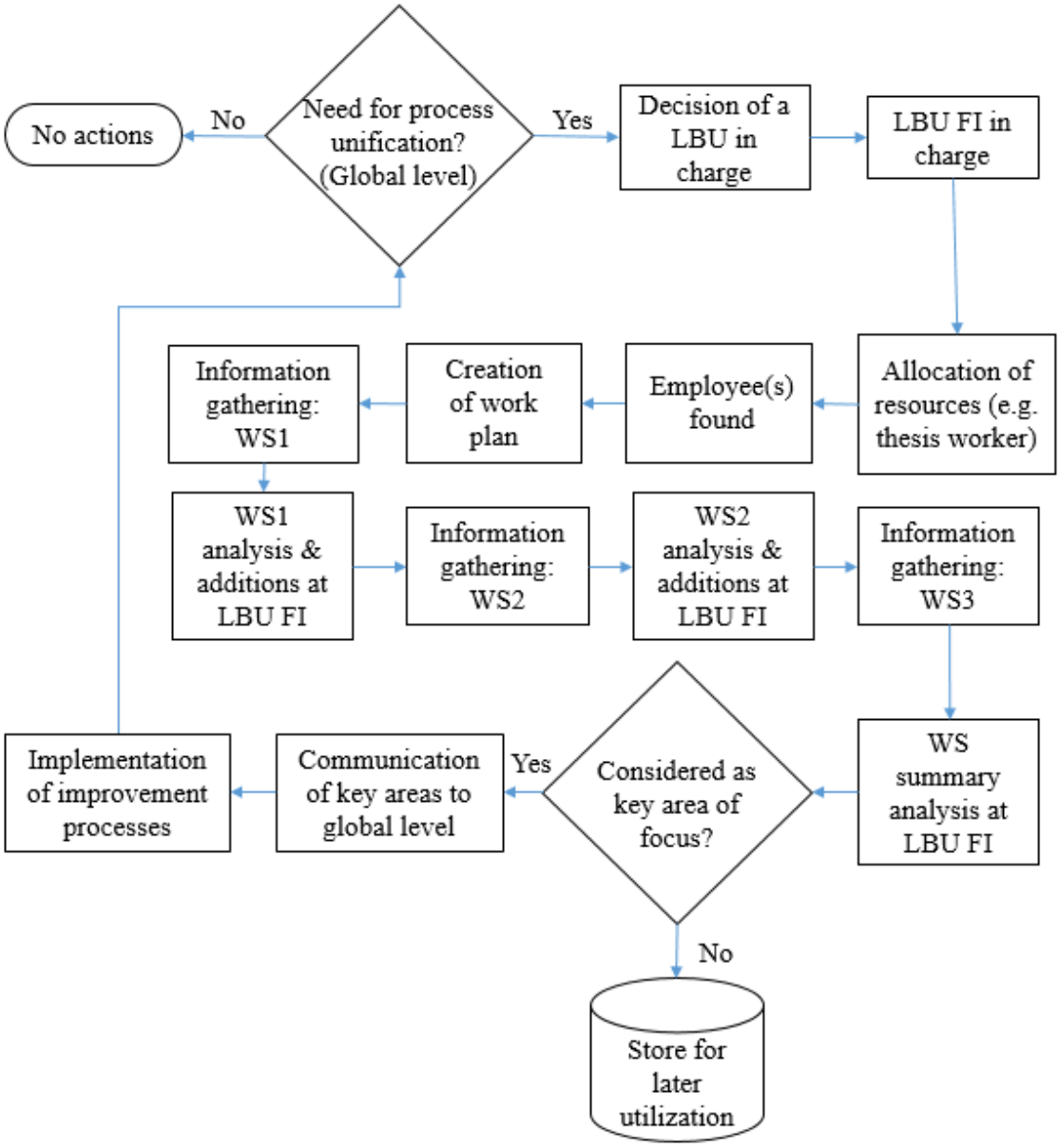


Figure 5: The overall process of global process unification

In Figure 5, the first processes are followed by the creation of a work plan, which in this example aims at information gathering through literature research and practical work at the company in the form of workshops with employees of different local business units. The workshops are presented in detail in the following chapter of this thesis and they represent different locations. After the first workshop (WS1), its outcome is analyzed at LBU FI and additions to the original agenda are made respectively. This way, in the second workshop (WS2), also the findings of the WS1 are analyzed. After the WS2, the information builds up through another analysis and additions at LBU FI. Finally, in the third workshop (WS3), not only the original agenda but the items raised in the previous

workshops and LBU FI analysis are processed and additional information value is gained. The number of the workshops may vary under different circumstances – it may be higher for example, but in this study, three workshops were desired as a starting point and to enable comprehensive analysis.

By summarizing all the gathered information and identifying the improvement areas with respective suggestions for improvement, decisions can be made: is the item considered as key area of focus or not? Cost benefit analysis and views of experts are supporting the decision making and prioritizing. If the item is not considered as key area of focus, it is stored for later utilization. The selected key areas of focus are then communicated to the global level. After this, the implementation of respective improvement processes requiring global cooperation can be started and finally, the very first decision can be reconsidered: is there still a need for global process unification? This leads to a continuous improvement cycle and storage of suggestions for improvement of lower priority, which can be at any time exploited.

3.2 Workshops

The first two-day workshop was organized by a product specialist of ABB Marine & Ports at ABB headquarter in Norway. This business unit's cybersecurity project execution process was chosen as the first one to investigate because it was commonly considered already well developed. The material collected from this workshop could this way serve as a base on which to build new best practices to share.

The topics discussed at the workshop in Norway included

- the cybersecurity team and respective roles,
- information sharing platform,
- cybersecurity process and project execution,
- technical solutions used for cybersecurity execution,
- cybersecurity standard documentation (internal and project delivery),
- quality control and follow up process and
- future plans, challenges and open questions of the Norway local business unit.

It was learnt, that although the business unit of Norway has its cybersecurity team, the roles of the members are not very official or standardized. For example, before the workshop, a clear diagram representing the flow of information and reporting between different departments and cybersecurity responsible persons did not exist. Also, some of the cybersecurity responsible persons may not be fully aware of their role, since it is controlled from the higher level, that they fulfill their responsibilities. However, the procedure exists and is ongoing – each project has its own named cybersecurity responsible person, a system engineer, reporting to "an integrator" that is following up and coordinating the cybersecurity execution of all the projects.

The business unit of Norway uses a Microsoft Sharepoint site as a platform to share information, procedures and news and to receive feedback from system users. Also, the follow up of the cybersecurity project execution process and an open task list are located at the Sharepoint site. The information sharing and especially feedback were seen as vital factors for effective cybersecurity execution – often improvements begin to happen based on the received feedback. What was discovered to improve the cybersecurity project execution process as well, was the standardization of documentation. Once different cybersecurity related documents, such as handover checklists and cybersecurity information document (including e.g. system IP addresses and SW and HW information), are made officially part of the project document delivery, they have to be and also are completed. When discussing the documentation, it was found out, that currently the cybersecurity testing is included in the system testing. It was considered, that the cybersecurity testing procedure should be standardized and a separate document should be generated to reflect it.

Other topics discussed at the workshop in Norway included the use of SW tools. Although they can be thought as to represent the technical details of cybersecurity and this way to be out of the scope of this thesis, it was discovered that they are a notable factor when improving cybersecurity. Effective use of SW tools can reduce engineering hours (for example during system configuration) dramatically by automating previously manually completed tasks. This way, the use of tools also reduces the risk of human error which is a significant cause of cyber incidents. The creation, testing and sharing of SW tools between different local business units should be given attention when making plans for cybersecurity improvements.

The human factor was discussed as an important topic of cybersecurity at the workshop in Norway. Different ways of raising cybersecurity awareness among employees and improving the current training methods were thought of. A common infrastructure and specific expert workshops were considered necessary. The technical knowledge, competence and procedures of ABB Marine were not seen as a major concern regarding cybersecurity – the key for improving and unifying the cybersecurity project execution process is in people's actions and harmonizing the ways to work in different locations.

The second workshop was implemented as a telephone conference with the technical product manager for cyber security services of ABB's Industrial Automation division, Control Technologies business unit, located in the Netherlands. The agenda and outcome of the workshop in Norway were used as a structure for the workshop, but the aim was to freely exchange ideas and get input from another business unit closely working together with ABB Marine. The cybersecurity role and responsibility division was discussed in the beginning of the workshop and it was assessed, if the cybersecurity responsible person of a project specifically needs to be a system engineer in the same way as at ABB Marine Norway. A possibility of a lead engineer taking responsibility of cybersecurity execution was seen as opportunity, depending on the competence of the person. The lead engineer

most likely could coordinate and assign the cybersecurity related tasks of the project without major difficulties. The interlocutor considered naming a cybersecurity responsible person for each project something potentially useful.

Another possible suggestion to improve the role definition that stood up during the second workshop could be nominating a common cybersecurity contact person for a local business unit answering both project related and internal questions. This has previously been done, but some problems occurred since it was an additional role for the contact person. The contact person had to complete the cybersecurity contact person tasks in addition to their regular work. Also, when solving project related issues, the cost allocation was simple, but when answering internal questions the contact person had to consult the management how much time can be used and holding the role became trickier. If something similar was desired in the future, it would be beneficial if the cybersecurity contact person was a full time employee in order to simplify the cost allocation and to enable full capacity for the problem solving. Basically, the division of cybersecurity roles and responsibilities highly depends on the available personnel and resources of the local business unit in question.

When discussing solutions for the cybersecurity follow up and maintenance during the project, the concept of the Sharepoint site of ABB Marine Norway was introduced to the interlocutor. The interlocutor shared their experience with the use of something similar, but explained problems related to that. A database for reporting issues and sharing information used to exist, but the use of it has slowly died. The interlocutor explained, that often, when new tools such as the previous database or the Sharepoint site are introduced to employees, the enthusiasm for using those lasts for a few months but the employees tend to not fully commit to it and the utilization slowly ends. The interlocutor also brought up, that in order to implement successful follow up, or more generally create alive and well working databases, it must be ensured that the employees are aware of how to correctly utilize them and it is important to get the users fully committed to the usage.

Also, in the second workshop the importance of standardizing the cybersecurity related project documentation was discussed. The writer of this thesis and the interlocutor agreed that the documents produced should be as simple and unambiguous as possible. Often, an expert becomes blind to themselves – when writing a document of a task they completed for example, they may not succeed in delivering text equally understandable for everyone regardless of their field of expertise. There is another problem related to the documentation, too. Unfortunately, many engineers do not necessarily enjoy writing documents. They may have even chosen their profession based on the presumably small amount of required writing. This sometimes becomes an issue, when the employee cannot, does not want to, or is not interested in producing good, valid text for others to read. For example, it would be very important to document details of system installations that require fulfilling specific customer requirements, but this has sometimes been failed to deliver. In order to succeed in the standardization of documentation, it is important to first design

good documents and then ensure that everyone delivering them understands them the same way and is able to fill the document accordingly.

The third workshop was implemented as a telephone conference with two cybersecurity responsible persons from the marine services focused local business unit of ABB Marine located in Italy. The previously introduced agenda and outcomes of the first two workshops were used as a base for the conversation. In the beginning of the workshop, the cybersecurity role and responsibility definition was discussed. In Italy, naming of specific cybersecurity responsible persons for projects is not completed. The business unit has one cybersecurity responsible person for the whole unit. Due to the smaller size of this unit, a strict role hierarchy is not seen necessary and the cybersecurity related information sharing is done by discussions. There are a lot of different positions filled by few people so flexible operation is required. In Italy, some organizational changes related to cybersecurity roles have been run and the definition of responsibilities is not very official or standardized.

The cybersecurity execution follow up and maintenance of Italy does not involve any platform such as the Sharepoint site of Norway. There is no central database for storing and sharing cybersecurity related information and the follow up consists of the delivery of required documents to the project leader, which means that the level of individual responsibility of completing required tasks is high. While discussing the documentation more generally, the interlocutors agreed with other locations that standardization of some sort would be beneficial. Also, the generation of wider documents including all the necessary cybersecurity related information was favored instead of having multiple different separate documents containing the same information. The perspective of the customer was also brought up: one of the interlocutors expressed that most likely the customer would like to see a single, informative document including all the necessary items rather than multiple different ones.

When discussing technical solutions for cybersecurity execution, the use of password management tools was focused on. It was discovered that multiple different external factors from global politics to the customer's opinion affect the choice of password management tool. In theory, the decisions on how to store passwords are made by ABB, but the customer owns the whole vessel and its systems and has the authority to choose how to proceed with password management. This may lead to complex situations in case the customer is responsible for managing all the passwords and this way has the authority to make changes to the systems – how can the warranty team of ABB Marine find out the root cause of any appearing problems, if the customer may have independently implemented any modifications out of the awareness of ABB Marine? The responsibilities should be clearly defined in order to ensure safety. The process of deciding on the password management tool in Italy is ongoing and ideally, each ABB Marine location could follow the same procedure or at least be aware of how to access any passwords in any situation.

During the third workshop, cybersecurity testing in wider scope was discussed. Current cybersecurity testing included in system testing mainly consists of double checking the configurations. In the future, for example wider use of penetration tests may be required by customers. Some of cybersecurity related items can be tested as part of system testing, but when considering cybersecurity on a larger scale, experts and a specific environment will be needed. ABB Marine has started the development of such environment. Other topic for the future development that was brought up was the importance of clarifying the company processes and defining the cybersecurity roles of different organization levels. Also, the human factor was highlighted – the attitude towards cybersecurity needs to get improved and it is a major challenge. Potentially, by demonstrating a clear way of earning value by cybersecurity, more positive attitudes towards it could be achieved.

3.3 Analysis of customer needs and expectations through project organization

Based on discussions with multiple members of ABB Marine project organization from different levels, the customer needs and expectations were analyzed. The topic was also discussed with the technical product manager for cyber security services of ABB Control Technologies business unit. A common opinion is, that the maritime industry is slowly increasing its cybersecurity awareness and execution levels and preparedness for cyber attacks. Cybersecurity is on customers' top agenda, but as in the whole process control industry, the development is relatively slow. Previously, cybersecurity execution and related solutions were considered rather fancy and not so closely relative to the industry. Also, the fact that vessels are physically moving and previously technically isolated from external sources may have had an influence on the slightly slower development of cybersecurity procedures and solutions – it has been seen at the same time as a challenge and not especially important. For example the oil and gas industry, partly because of its more stationary characteristics, is far ahead in its cybersecurity execution and solutions compared to the maritime industry. Now, the attitudes of the maritime industry have started to change and the customers are requiring effective cybersecurity execution – and this requires adjustments from ABB Marine & Ports as well. Also, some actors such as the classification society DNV GL have already announced, that during 2018 its newly released cybersecurity recommendations will change into rules.

A question and challenge ABB Marine is facing is how to provide cybersecurity improving service, such as SW updates after the delivery of the vessel and get the customer committed to it? Remote access platform offers a solution to this and the customers generally favor the idea, but they also want to feel safe. Remote access is still seen as a notable threat since it may be the only point of access from the vessel to the internet and this way presents a major vulnerability. Also, not all the customers are fully comfortable with the technology nor willing to pay for it yet. The customer often does not want anyone from the outside of the vessel to access their system or make any modifications to setups.

An important factor when convincing the customer of remote diagnostic services is to highlight the fact that ABB Marine remote diagnostic system is a read-only system and to get the customer to see that the data they are sharing is used exclusively for their benefit.

Also the fact, that cybersecurity solutions can be thought as an insurance make the convincing of the customer even more challenging. When compared to for example an industry solution that forecasts and optimizes production of some sort, it is way more effortless to prove the effectiveness of the solution when solid statistics of the results of using the solution exist. A cybersecurity solution on the other hand is something the customer invests in and pays for – and potentially never sees the effect in a similar, measurable way as for example a certain percentage of energy savings. The value that the cybersecurity adds should be more clearly demonstrated to the customers. The convincing should base on real experience sharing – not theoretical papers nor marketing material. Also, if classification societies placed direct requirements for new solutions it would facilitate the customer assurance to show compliance with these requirements. This is something to be prepared for in the future. There are no common cybersecurity rules to show compliance with and refer to, yet. Currently, how the customer reacts to new solutions highly depends on the personality being faced.

Another factor affecting the customer's attitude towards remote services is what the vessel is loaded with – is it transporting cargo only or are there large amount of people, such as cruise ship customers onboard? In case of cruise ships, the risk of harming or losing life is greater and such risks are often considered extremely critical. However, the slow change in attitudes towards positive can be seen and ABB Marine has already managed to make update service contracts. Generally, the customers of newbuilding projects are more interested in the new solutions since these systems are easier to build from scratch. The customers tend to be rather reactive, not proactive, what it comes to updating of systems and adapting new solutions. When nothing is broken, it is not seen important to consider updates or new solutions. A significant amount of vessels still run computers with old operating system versions. Updating computers and an already existing infrastructure can be difficult, laborious and costly. Another challenge faced when convincing customers of new solutions is connected to ethics – in the most radical case, the potential new, advanced solutions may lead to loss of jobs and this is an issue the customer needs to consider. Nevertheless, ABB Marine needs to continue preparing for the growth in demand of remote SW updates and other cybersecurity improving services and offer solutions to fulfill this demand.

3.4 Cybersecurity project execution process improvement area detection

In this chapter, improvement areas found in ABB Marine's cybersecurity requirements and cybersecurity project execution process are identified based on the previous literature and industrial practices review section and the outcome of the workshops. ABB Marine has a formal cybersecurity organization, which has the mandate and authority to enforce the company's cybersecurity requirements for products, project deployment and service, as well as for the company's suppliers. ABB addresses cybersecurity throughout the entire lifecycle, beginning from the design of the product, including all the phases through commissioning until the maintenance, review and upgrade of the product. For example, the "ABB Cyber Security Requirements for Suppliers" (2017c) presents requirements for suppliers from 12 areas: secure development lifecycle, security quality, backdoor accounts and hardcoded credentials, cryptographic tools and security functionalities, protection from malware propagation, handling of digital certificates, product documentation, vulnerability handling, patch management, software integrity and authenticity, data collection, and sub-suppliers and sub-contractors. In a similar way, ABB Marine sets requirements for its products, projects and services.

During the investigation and comparison of the findings of the literature and industrial practices review, outcome of the workshops and ABB Marine's cybersecurity requirements for projects, following improvement areas were detected:

- Inadequate global infrastructure and standardized cybersecurity project execution process for different local business units: different business units have created their own processes.
- Inadequate standardized cybersecurity related documentation: different local business units are producing documentation with the same contents, but different forms.
- Unclear definition of cybersecurity roles and responsibilities: the traceability chain is incomplete and especially the reporting may not proceed to the top level.
- Conflicts between global and local cybersecurity guidelines: for some products, contradictory guidance from different levels is provided.
- Information sharing and collection of feedback, also from the customer, is insufficient.
- The lack of separate, standardized cybersecurity testing procedure: currently, the cybersecurity testing is included in system testing.
- Awareness and attitudes: tasks tend to be completed with precision only when they are standardized and officially required.
- Training: not seen as a major concern, but room for improvement still exists – training is not globally valid.

- Technical solutions and procedures for cybersecurity execution: solutions are not produced, tested and shared in a coordinated manner; inadequate global lifecycle management.

3.5 Key areas of focus for the unification of cybersecurity process

In this chapter, potential solutions and suggestions for improvement of the previously identified cybersecurity project execution process improvement areas are presented. Out of these, the key areas of focus for ABB Marine from which to begin the unification of cybersecurity execution and maintenance process for projects are identified. One of the goals of this thesis was to assess the topic comprehensively – without seeing the big picture first, important factors may have been missed during decision making and focus might have been put on less necessary areas. This is why the research aimed at the definition of the key areas. The process unification can be launched effectively, when the most critical areas are first commonly identified.

Table 3 presents the detected improvement areas and the suggestions for improvements in compressed form. In the next paragraph, the contents of the table are discussed in more detail.

Improvement area	**Suggestion for improvement**
Inadequate global infrastructure and standardized cybersecurity project execution process	Enhancing of a common global level Sharepoint site
Inadequate standardized cybersecurity related documentation	Converting unofficial documents to standardized ones with ABB document numbers
Unclear definition of cybersecurity roles and responsibilities	Naming a cybersecurity responsible person in each project, clarifying the information flow between different actors
Conflicts between global and local cybersecurity guidelines	Clarifying the priority: global guidelines must be followed; locally additional measures can be taken, but the responsibility of those and the maintenance moves to the local level
Insufficient information sharing and feedback collection	Sharing information and collecting feedback through the Sharepoint site

Lack of separate, standardized cybersecurity testing procedure	Contacting ABB testing center in order to begin the establishment of a standardized cybersecurity testing procedure
Awareness and attitudes Training	Organizing expert workshops and "technical lunch" sessions Developing globally valid training, improving web training by adding video material
Technical solutions and procedures for cybersecurity execution	Standardizing on one global password management tool; establishing a standardized production, testing and sharing procedure for cybersecurity improving technical solutions; improving backup storage to complement global lifecycle management

Table 3: Identified cybersecurity project execution process improvement areas and suggestions for improvement

A large part of the identified improvement areas relate to inadequate standardization and problems with information sharing. The Sharepoint site created at the business unit of Norway could be expanded to global level use. This would be relatively painless to implement and it would be a solid starting point for the development of a common infrastructure. The Sharepoint site would be the main channel for cybersecurity related information sharing between local business units – also feedback from projects could be collected and announcements made through this channel. Open task and follow up lists could be maintained, the cybersecurity project execution process (or a few alternatives for different project types) could be described and the cybersecurity related project documents could be stored at the Sharepoint site. The continuous follow up of cybersecurity related activities during all the phases of the project is seen as a specific area of development. Currently, the cybersecurity handover audit before the warranty phase is subject to a lot of pressure. More continuous follow up, such as milestone based approach, stored at the Sharepoint site for example might improve the situation. The challenge in the implementation of a global Sharepoint site is to get employees committed to using it.

The Sharepoint site would increase the traceability of actions also by making the cybersecurity responsible persons more visible. The roles of these persons, the information flow and responsibilities should be clarified. In Norway, a procedure for this exists and a similar idea could be applied to ABB Marine Finland. In this case, the resources need to be carefully considered. In Norway, the cybersecurity responsible person of a project is

invariably a system engineer. In Finland, other options can be considered – the same responsibility could be undertaken by the lead engineer of a project, for example. Also, in Norway, these cybersecurity responsible system engineers report to one higher level "integrator", which takes care of the follow up and reports to the higher, global level. It is still unknown, if the business unit of Finland would be able to name a similar type of an integrator, but investigations on this have been started. Another open question also is, whether the global level reporting is fully utilized or not. To be effective, the reporting should continue without any bottlenecks in order to ensure that the information can actually be used.

In the documentation, creation and use of unofficial documents should be avoided. It has been found, that once the document is official, it has been appointed an ABB document number and it is part of the project document delivery set it is often more carefully filled out. This way, there is no question nor choice – the document needs to be created and its contents need to properly be fulfilled. Currently, different local business units are producing documents with similar contents but in different forms. For example, some units prefer documents with more contents while the others divide these same contents in multiple different documents. It would be beneficial, if a standardized way was followed in different units.

Some conflicts between global and local level guidelines exist. Their priorities should be clarified. For a global product, global guidelines should at all times be followed. In some cases, more detailed or strict local guidelines and measures have been established. These can be practiced, but it should be clear, that the responsibility of the measure in question moves to the local level. For example, use of managed network switches is not always necessary, but in case these are chosen to be used, the local team is in charge of them. The conflicts between global and local guidance should be broken down and the influence of local units to the cybersecurity requirements of global products should be clarified and communicated to local teams.

Currently, cybersecurity testing is included in the system testing. A need of a separate, standardized cybersecurity testing procedure has been identified. During this thesis, the preparation and building of a cybersecurity laboratory was started. In order to begin the development of the testing procedure, the ABB testing center should be contacted. Also, the production, testing and sharing of technical solutions such as SW tools for cybersecurity execution is insufficient. A standardized procedure for this should be developed. The software team should be contacted to begin the process. It was also discovered, that different locations use different password management tools. The reason for this should be further investigated and the use of a common, globally used password management tool should be pursued.

There is no single globally effective method for improving cybersecurity related awareness, attitudes and training, but the need for expert workshops was identified. Expert

workshops would offer a chance for more effective information sharing than simple cybersecurity status meetings that currently exist. However, the organization of expert workshops is quite resource-consuming so only limited possibilities for them exist. Existing web training could be updated for example to include video material in order to make the training more attractive to the employees. Another method for improving awareness, attitudes and training could be a "technical lunch" session. During these sessions, an employee from certain area of expertise delivers a presentation of a desired topic while the audience members enjoy their lunch. These sessions would be organized during the lunch break to lower the participation threshold and invitations would be sent to every employee that the subject may touch. Technical lunch sessions have already been proven effective in Norway so this may be something to consider in Finland as well.

It was also discovered, that different locations have slightly different cybersecurity training requirements for their employees working in projects. Generally, the same collection of web courses needs to be taken, but in Finland, an additional "hands-on" session is required for everyone working close to the systems of a vessel. In theory, this leads to the situation where for example a project engineer from Norway would not be qualified to work in projects of Finnish ownership. To increase the flexibility of using employees from different business units globally, the training should be standardized – a reasonably resource efficient solution would be adding the hands-on session as a part of the cybersecurity training in other locations as well.

3.5.1 Selecting key areas of focus for the process unification

In this chapter, the reasoning for the selection of key areas of focus for the process unification is presented and finally, the selected key areas are listed. The whole research was done with one important factor in mind – at ABB Marine Finland, the technical cybersecurity related knowledge, measures and procedures were not seen as major concern. To a large extent in practice, cybersecurity execution can be thought to consist of access limitation and isolated systems. The company believes that the technical measures and procedures for effective cybersecurity execution from this point of view exist. It would be more important to ensure that everything else on a larger scale supports these already existing and effective measures rather than focusing on the technical details too much. This is why the research concentrated on the project point of view.

When selecting the key areas of focus for the process unification, ABB Marine Finland needs to consider which issues it can truly affect, which generally mean the company's own actions. It may be beneficial to try influencing the customer's actions for example in order to make the customer interface smoother. It is also important to be aware of the division of cybersecurity responsibilities between ABB and the customer. However, from the perspective of this research, focus on ABB Marine Finland's own actions was kept. Another important factor for the selection of key areas was the cost benefit ratio. Also

purely from the cybersecurity point of view, only cost and resource efficient improvements with the highest positive effect on cybersecurity should be implemented.

ABB Marine Finland will work for the improvement of all the improvement areas of Table 3, but prioritizes the following items:

- **Inadequate global infrastructure and standardized cybersecurity project execution process**: The enhancing of a common global level Sharepoint site was started in global cooperation with the local business unit of Norway's cybersecurity Sharepoint admin.
- **Training**: A goal was set, that employees from different local business units could work in any other location's projects by completing a common set of training.
- **Conflicts between global and local cybersecurity guidelines**: The clarification process was started for the Remote Diagnostic System product in global cooperation with the global product manager, automation infrastructure product area manager and other relevant experts.
- **Technical solutions and procedures for cybersecurity execution**: The process of deciding on a global password management tool was started. The development of a new cybersecurity execution service solution was started in global cooperation with system, cybersecurity service and other relevant experts.

The common global level Sharepoint site was considered as a good starting point and basis for the unification process of cybersecurity project execution. Only the fact that cybersecurity related information from all the locations is collected together and visible for all relevant employees in a structured and coordinated way may speed up the unification and interaction between different locations. The enhancing of the global Sharepoint site was started as a result of the workshop in Norway and the following discussions. The already existing cybersecurity Sharepoint site of Norway was used as a base for the new, global one and technical documentation specialists were consulted in order to ensure the best possible implementation. Additionally, following the workshop in Norway and this thesis work, ABB Marine & Ports began considering its cybersecurity role and responsibility division and specifically the need for naming a globally responsible person for cybersecurity project deployment. This enables effective development and maintenance of the new, global level cybersecurity Sharepoint site. The identified improvement areas can this way be improved in global cooperation. The writer of this research continues supporting the process after returning the thesis.

It was seen possible to improve cybersecurity training in a reasonably budget friendly and little resource consuming way. The clear differences between the training requirements of different locations can be faded by complementing the lower sets of requirements with the existing higher ones – in this case, by adding the hands-on training session to all locations. The current hands-on training needs to be studied in order to find out the best way to implement the same contents in different locations. The investigation was started

as a result of this research. Additionally, cybersecurity training is a topic demanding careful consideration in the future. The cybersecurity standardization process in a large scale is running and industries are agreeing on common rules and requirements. This will eventually lead to the stabilization of the status of cybersecurity training similar to the existing occupational safety, hot work and safety at electrical work trainings – without a completed, nationally valid course, a person is not qualified to work in an environment requiring those courses. A more formal status of this kind potentially increases the level of cybersecurity awareness as well once the organizing of necessary training for employees is not only in the hands of the company in question but an absolute, national requirement.

Conflicts between global and local cybersecurity guidelines must be clarified. The issue was revealed, when the global product manager of the Remote Diagnostic System of ABB Marine & Ports contacted the writer of this thesis and presented the feedback received from different local teams. When addressing the issues in Finland, it was found out that problem solving will require participation of experts from different areas. The process started from reviewing one specific product, but soon expanded to larger scale involving consideration of other products and the entity they form. Also, group level globalization of security policies is currently running. The clarification process will continue in global cooperation after returning this thesis and the writer will remain involved.

The consideration of technical solutions and procedures for cybersecurity execution raised the question of password management tools in use. The harmonizing of the use of password management tools was started in order to ensure successful service operations regardless the location in question. Additionally, as a result of this thesis, the development of a new cybersecurity improving service solution was started in global cooperation. At the workshop in Norway, the host of the workshop expressed a need for implementing an already existing solution for large scale systems. This has not been completed before, but the resources for the implementation existed. Following the workshop and discussions in Finland, the writer of this thesis contacted the global cyber security solution manager of ABB Marine & Ports and the development process was kicked off involving the relevant specialists. After returning this thesis, the writer continues assisting in the process.

3.5.2 Additional future suggestions

This chapter presents other observations and ideas of the writer for the future based on the literature and industrial practices review and the practical work done for this research. The writer sees the definition of cybersecurity roles and responsibilities inside organizations as an extremely necessary matter. These roles and responsibilities are not fully settled as common standard and routine among the companies yet – although the full concept of cybersecurity may be part of the company's overall management, deficiencies in the organizing of the cybersecurity responsibilities can be found. This can however be slightly compensated by the responsibility of the individual which is essential for effec-

tive overall cybersecurity execution and requires high level of awareness and commitment. During the research, the writer found out that also the cybersecurity organization of ABB Marine is continuously evolving. New roles will be defined which is a good direction on the way of fulfilling all cybersecurity needs and ensuring effective, continuous development of overall cybersecurity and cyber risk management. Clear definition of roles and responsibilities also facilitates the flow of information, which often, when insufficient, has been noted to cause problems.

Compliance with the newest cybersecurity best practices, frameworks and cyber programs presented in the literature and industrial practices review may be proved very important for ABB Marine when seeking competitive advantage in the future. It will be mandatory for ABB Marine to fulfil some of the current recommendations in the near future when they become rules, as for example DNV GL has already announced. This is a minimum requirement – by doing more, for example when demonstrating compliance with the new, potentially ad hoc standard NIST Framework for Improving Critical Infrastructure Cybersecurity (2017), additional benefits can be achieved. Also the ABS CyberSafety™ series (2016) attracted the writer's interest as the maritime "industry's first risk-based management program". Certification of compliance of this kind of holistic maritime cyber risk management program is a solid proof for customers of advanced cybersecurity maturity. Such certifications could potentially be a way for ABB Marine to stand out from the competitors and attract new markets. Pioneering in the area of cybersecurity as well is necessary for ABB Marine in order to ensure growth in the future. The company also needs to be able to demonstrate that its new, cyber-enabled solutions are safe and add value when marketing them – they are key factors when convincing the customer. New cybersecurity certifications offer this opportunity and may be worth further investigation.

4. CONCLUSIONS AND FUTURE WORK

This thesis provides a literature and industrial practices review of the latest cybersecurity publications of the maritime industry and in practice, presents a methodology for global process unification and identifies the key areas of focus for ABB Marine Finland from which to begin the unification of their cybersecurity execution and maintenance process for projects. This chapter summarizes the findings and the results of the research, evaluates them and briefly proposes topics for future research.

4.1 Key findings and results

The literature and industrial practices review demonstrated the ruling approach of the maritime industry for cybersecurity – holistic cyber risk management through each organization level. The maritime sector has defined the need for common cybersecurity standardization and currently actively works towards this. Different actors of the industry, such as classification societies, are frequently publishing their cybersecurity best practices which are expected to become rules in the near future, some even during 2018. The cybersecurity framework by NIST (2017), although currently published as draft version, is already frequently referred to and recognized by the maritime industry. In order to gain competitive advantage, ABB Marine has to fill all the new cybersecurity requirements without delay. The introduction of new cybersecurity certifications, such as the ABS CyberSafety™ series (2016), may increase these requirements in case they are considered valuable and worthy of pursuit.

In addition to providing a literature study, this thesis aimed at improving the cybersecurity execution process for projects at ABB Marine. Currently, differences between local business units can be found. The company has recognized the need for unifying their cybersecurity execution and maintenance process for projects towards single, global level process. Since the unification process is extensive, the goal of this thesis was to identify the key areas for the beginning of the work. The literature and industrial practices review was used as a theoretical framework for the empirical part consisting of workshops with cybersecurity responsible persons of the company and the following analysis of this thesis.

By investigating and comparing the findings of the literature research, outcome of the workshops and ABB Marine's cybersecurity requirements for projects, a list of cybersecurity project execution process improvement areas and relative suggestions for improvement was presented. All the detected improvement areas will be worked on, but ABB Marine Finland prioritizes items from four key areas: inadequate global infrastructure and standardized cybersecurity project execution process, training, conflicts between local

global and local cybersecurity guidelines and technical solutions and procedures for cybersecurity execution.

Following this thesis, ABB Marine Finland decided to begin enhancing of a common global level Sharepoint site which was considered to be a solid start for the process unification. A common Sharepoint site improves information sharing, collection of feedback and common infrastructure, when relevant cybersecurity information is visible for all locations under single platform.

Training was selected as another key area for process unification. ABB Marine Finland set the target of standardizing the cybersecurity training to be globally valid in such way, that employees from different local business units could work in any other location's projects. This can be implemented by adding the contents of the business unit of Finland's hands-on session to the training in other locations. The investigation on the best way to implement this and the search for potential new responsible persons for training was started.

As a result of this thesis, a clarification process of conflicting global and local cybersecurity guidelines started. The issue was revealed when reviewing the Remote Diagnostic System product, but now involves consideration of other products, the entity they form and participation of experts from different areas.

For the technical solutions and procedures item, ABB Marine Finland began investigating the potential use of a global password management tool. This would ensure successful operations in any location. Also, the development of a new cybersecurity execution service solution was started in global cooperation following the workshop in Norway.

This thesis kicked off definition of new cybersecurity roles for ABB Marine & Ports. Designation of a globally cybersecurity responsible person for project deployment is planned. The development of standardized cybersecurity best practices was considered so necessary that ABB Marine Finland is also considering the recruitment of a new, full time employee for cybersecurity. In addition to the previously presented cybersecurity development processes, the writer of this thesis will continue supporting the improvement of cybersecurity in the company after this thesis.

4.2 Evaluation of research results

Overall, this thesis succeeded in answering the research questions, but some challenges were faced during the process. This chapter evaluates the results of the research and their theoretical and practical relevance.

This thesis represents new type of research for ABB Marine & Ports and more generally, to the maritime sector. Cybersecurity is a hot topic for the whole industry and this research aimed at collecting together the current approaches of different actors of the maritime

sector in the literature and industrial practices review. This was successful, but due to the scope of this thesis, the most detailed examination of the material was not carried out and may be considered necessary in the future. New cybersecurity related publications are also continuously being released and in order to stay up to date, the company needs to follow release channels and investigate all the relevant, new guidelines. However, the literature and industrial practices review provides for example the management and cybersecurity responsible persons of the company with a versatile overview of the current cybersecurity situation of the maritime industry. It may also help the preparation for future requirements.

Practically, the participation of experts from different areas in the contribution of this thesis adds the reliability and validity of the results. The research was done from ABB Marine project organization's perspective and the writer managed to cooperate with cybersecurity responsible persons from different local business units. In the scope of the research, the experts represent the project organization sufficiently and provided reliable information. All the experts argued their views carefully which enabled comprehensive analysis and comparison of different options. The count of the participating experts could potentially have been higher, but in that case such thorough discussions may not have been possible.

The fact that solving cybersecurity related issues often is an additional activity of the experts' job description caused some challenges in the process. Finding the time and resources for the participation required careful planning, but despite the limitations even face to face meetings were successfully organized. Realizing this, the time with experts was well planned and efficiently used. Although the topic of cybersecurity was widely addressed, same issues emerged in different conversations. This validated the common view about which items are important. The decision making and prioritization of different items proved to be challenging, but this was managed by analyzing which items would be relatively effortlessly realizable, cost efficient and offer immediate, tangible benefits. The list of improvement areas and suggestions for improvement produced in this thesis acts as such as a tool for developing the cybersecurity policies and procedures of the company. This thesis provides practical suggestions for the cybersecurity related issues the project organization of ABB Marine & Ports is facing but in order to ensure the successful further development, the unification process continues under the group level globalization of security policies.

4.3 Further research topics

The topic of this research is extensive and still leaves a need for future research. In order to ensure the successful unification of cybersecurity execution and maintenance process for projects, ABB Marine needs to study more closely at what level the unification is possible. The special features, requirements and distinctive forms of business of different

local business units need to be carefully considered. The unification process requires global cooperation on all levels of the organization.

Since the literature and industrial practices review of this thesis provides an overview of the selected sources, ABB Marine needs to decide whether some of the publications require special attention and examination in the future. Material produced by the closest stakeholders of ABB Marine & Ports may need more detailed and systematic exploring in order to ensure full compliance. Also, the potential value of new cybersecurity certifications, such as the ABS CyberSafety™, may need to be investigated.

The maritime industry's future direction towards the increased amount of cyber-enabled solutions and autonomous vessels demands ABB Marine to remain up to date with the newest cybersecurity requirements and rules of the industry. In order to successfully bring new products to the market, these requirements must be fulfilled and this must be demonstrated to the classification societies, customers and other stakeholders. In the future, the topic of cybersecurity will increase its significance in the maritime sector and when the customers are adapting to the change of the industry, ABB Marine needs to answer these needs promptly in order to achieve competitive advantage.

REFERENCES

ABB Cyber Security, ABB Group Cyber Security Council, 2016, 30 p.

ABB Cyber Security Requirements for Suppliers, ABB, Version 1.0, 2017c, 5 p. Available (19.9.2017): http://search.abb.com/library/Download.aspx?DocumentID=9AKK106930A4400&LanguageCode=en&DocumentPartId=&Action=Launch

ABB Facts and Figures, ABB, 2017a, Available (28.9.2017): http://new.abb.com/investorrelations/company-profile/facts-figures

ABB Oy, Marine & Ports, Energiatehokasta merimatkaa, 2017b, Available (28.9.2017): http://new.abb.com/fi/abb-lyhyesti/suomessa/yksikot/marine-and-ports

Cybersecurity – Guidance Notes for the Marine and Offshore Industries, American Bureau of Shipping, 2016, 8 p. Available (24.8.2017): https://ww2.eagle.org/content/dam/eagle/publications/2016/Cybersecurity_16053_LR.pdf

CyberSafety™ – Volume 1: Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations, American Bureau of Shipping, 2016, 45 p. Available (24.8.2017): https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf

CyberSafety™ – Volume 2: Guide for Cybersecurity Implementation for the Marine and Offshore Industries, American Bureau of Shipping, 2016, 118 p. Available (24.8.2017): https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/251_cybersafetyV2/CyberSafety_V2_Cybersecurity_Guide_e.pdf

The Guidelines on Cyber Security Onboard Ships, Baltic and International Maritime Council, Version 2.0, 2017, 36 p. Available (27.7.2017): https://www.bimco.org/news/press-releases/20170705_cyber-g

BSI IT-Grundschutz Catalogue, Bundesamt Für Sicherheit in der Informationstechnik, 13. Edition, 2013, 4220 p. Available (23.8.2017): https://download.gsb.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf

Cybersecurity of Connected Vehicles – Best Practices, Bureau Veritas, 2016, 40 p. Available (13.9.2017): http://www.bureauveritas.com/white-papers/Cyber-security-of-connected-vehicles-Best-practices

H. Boyes & R. Isbell, Code of Practice – Cyber Security for Ships, Institute of Engineering and Technology, 2017, 73 p. Available (19.9.2017): https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf

Definition of Cybersecurity, Focus Group on Cybersecurity, European Committee for Standardization/European Committee for Electrotechnical Standardization, Version 1.08, 2016, 57 p. Available (19.8.2017): ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/Security/CybersecurityDefinition%20v1.1.pdf

Recommended Practice – Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation, DNV GL, 2016, 86 p. Available (10.8.2017): https://www.dnvgl.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html

Analysis of Cyber Security Aspects in Maritime Sector, The European Union Agency for Network and Information Security, 2011, 31 p. Available (19.8.2017): https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

IEC 61162-460:2015, Maritime Navigation and Radiocommunication Equipment and Systems – Digital Interfaces – Part 460: Multiple Talkers and Multiple Listeners – Ethernet Interconnection – Safety and Security, International Electrotechnical Commission, 2015, 62 p. Available (20.9.2017): https://webstore.iec.ch/publication/23120

IEC 61508:2010, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems – Parts 1 to 7 together with a Commented Version, International Electrotechnical Commission, 2010, 1000 p. Available (20.9.2017): https://webstore.iec.ch/publication/22273

IEC 62443 series of standards for Industrial Automation and Control Systems Security, Parts 1 to 4, International Electrotechnical Commission 2016. Available (20.9.2017): http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx

IEC 62443-3-3:2013, Industrial Communication Networks – Network and System Security – Part 3-3: System Security Requirements and Security Levels, International Electrotechnical Commission, 2013, 80 p. Available (20.9.2017): https://webstore.iec.ch/publication/7033

IEC 62443-4-2, Security for Industrial Automation and Control Systems – Technical Security Requirements for IACS Components, Draft Version, International Electrotechnical Commission, 2017, 90 p. Available (20.9.2017): http://isa99.isa.org/Public/Series/Documents/ISA-62443-4-2-Public.pdf

Guidelines on Maritime Cyber Risk Management, International Maritime Organization, The 98th Maritime Safety Committee, 2017, 6 p. Available (10.8.2017): http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

COBIT 5 Introduction, ISACA, 2012, 45 p. Available (21.9.2017): https://www.isaca.org/COBIT/Documents/COBIT5-Introduction.ppt

The Standard of Good Practice for Information Security 2016, Executive Summary, Information Security Forum, 2016, 3 p. Available (21.9.2017): https://www.securityforum.org/uploads/2016/07/SoGP-2016-Exec-Summary-FINAL-260716.pdf

ISO 10007:2017, Quality Management – Guidelines for Configuration Management, International Organization for Standardization, 2017, 10 p. Available (20.9.2017): https://www.iso.org/standard/70400.html

ISO 26262, Road Vehicles – Functional Safety, Parts 1 to 9, International Organization for Standardization, 2010.

ISO 9000:2015, Quality Management Systems – Fundamentals and Vocabulary, International Organization for Standardization, 2015, 51 p. Available (20.9.2017): https://www.iso.org/standard/45481.html

ISO 9241-210:2010, Economics of Human-System Interaction – Part 210: Human-Centred Design for Interactive Systems, International Organization for Standardization, 2010, 32 p. Available (20.9.2017): https://www.iso.org/standard/52075.html

ISO/IEC 15408-1:2009, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Model, International Organization for Standardization, 2009, 64 p. Available (20.9.2017): https://www.iso.org/standard/50341.html

ISO/IEC 15408-2:2008, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 2: Security Functional Requirements, International Organization for Standardization, 2008, 218 p. Available (20.9.2017): https://www.iso.org/standard/46414.html

ISO/IEC 15408-3:2008, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security Assurance Requirements, International Organization for Standardization, 2008, 174 p. Available (20.9.2017): https://www.iso.org/standard/46413.html

ISO/IEC 27000:2014, Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary, International Organization for Standardization, 2014, 30 p. Available (20.9.2017): https://www.iso.org/standard/63411.html

ISO/IEC 27000:2016, Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary, International Organization for Standardization, 2016, 34 p. Available (20.9.2017): https://www.iso.org/standard/66435.html

ISO/IEC 27001:2013, Information Technology – Security Techniques – Information Security Management Systems – Requirements, International Organization for Standardization, 2013, 23 p. Available (20.9.2017): https://www.iso.org/standard/54534.html

ISO/IEC 27002:2013, Information Technology – Security Techniques – Code of Practice for Information Security Controls, International Organization for Standardization, 2013, 80 p. Available (20.9.2017): https://www.iso.org/standard/54533.html

M. Lehto & A. Kähkönen, Kyberturvallisuuden kansallinen osaaminen, Jyväskylän yliopisto, 2015, 58 p. Available (19.9.2017): https://www.jyu.fi/it/tutkimus/202015_Kyber_kansallinen_osaaminen_VERKKO.pdf/view

J. Limnéll, K. Majewski & M. Salminen, Kyberturvallisuus, Docendo Oy, 2014, 246 p. ISBN 978-952-291-047-9.

Cyber-enabled Ships – Deploying Information and Communications Technology in Shipping – Lloyd's Register's Approach to Assurance - Guidance Note, Lloyd's Register, 1. Edition, 2016, 20 p. Available (27.7.2017): http://www.lr.org/en/services/cyber-technology-for-marine.aspx

Cyber-enabled Ships – ShipRight Procedure – Autonomous Ships – Guidance Document, Lloyd's Register, 1. Edition, 2016, 31 p. Available (21.8.2017): http://www.lr.org/en/services/cyber-technology-for-marine.aspx

Federal Information Processing Standards, Publication 199, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, 2004, 13 p. Available (4.8.2017): http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, Draft Version 1.1, 2017, 61 p. Available

(26.7.2017): https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

J. Jorgensen, ABS CyberSafety™, SOCP Webinar, 2016, 19 p. Available (20.9.2017): http://www.socp.us/images.html?file_id=40UY2UEl78k%3D

B. Segalis, A. Rudawski, US Coast Guard Releases Draft Cybersecurity Guidelines, Data Protection Report Blog, 2017. Available (14.9.2017): http://www.dataprotectionreport.com/2017/07/us-coast-guard-releases-draft-cybersecurity-guidelines/

L. Shen, The NIST Cybersecurity Framework: Overview and Potential Impacts, Scitech Lawyer, American Bar Association, Vol. 10:4, 2014, 16-19 pp.

K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams & A. Hahn, NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology, Revision 2.0, 2015, 247 p. Available (20.9.2017): http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

A. Terroza, Information Security Management System (ISMS) Overview, The Institute of Internal Auditors, 2015, 30 p. Available (20.9.2017): https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf

Cyber Strategy, United States Coast Guard, 2015, 44 p. Available (14.9.2017): https://www.uscg.mil/SENIORLEADERSHIP/DOCS/cyber.pdf

Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities, United States Coast Guard, 2017, Draft Version, 37 p. Available (14.9.2017): http://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/DRAFT%20Cyber%20NVIC%2005-17.pdf?ver=2017-07-19-070240-737

44 U. S. Code, Section 3542, Definitions, 2002. Available: https://www.gpo.gov/fdsys/granule/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542

APPENDIX A: THE ABS CYBERSAFETY™ FULL CAPABILITY MODEL

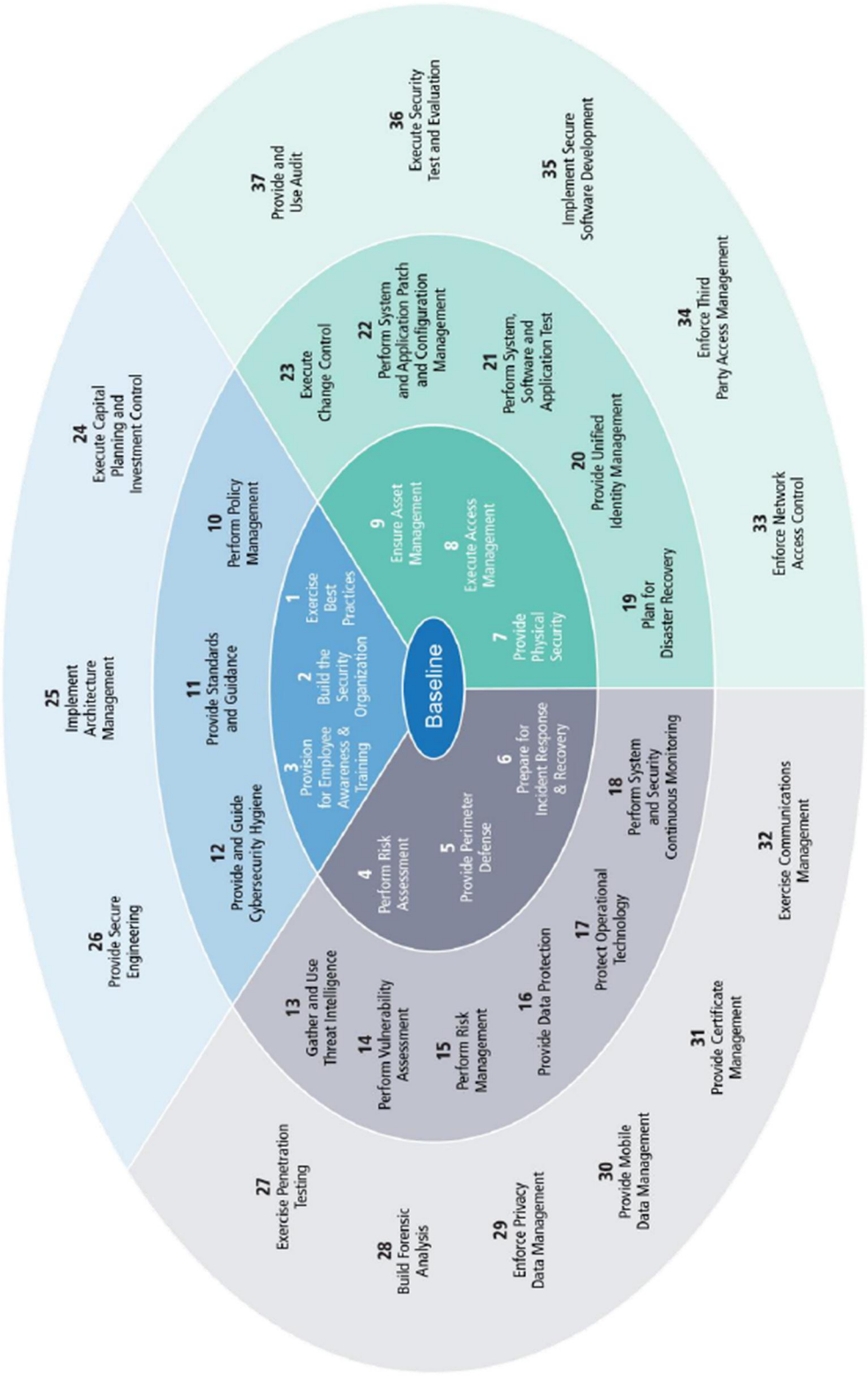
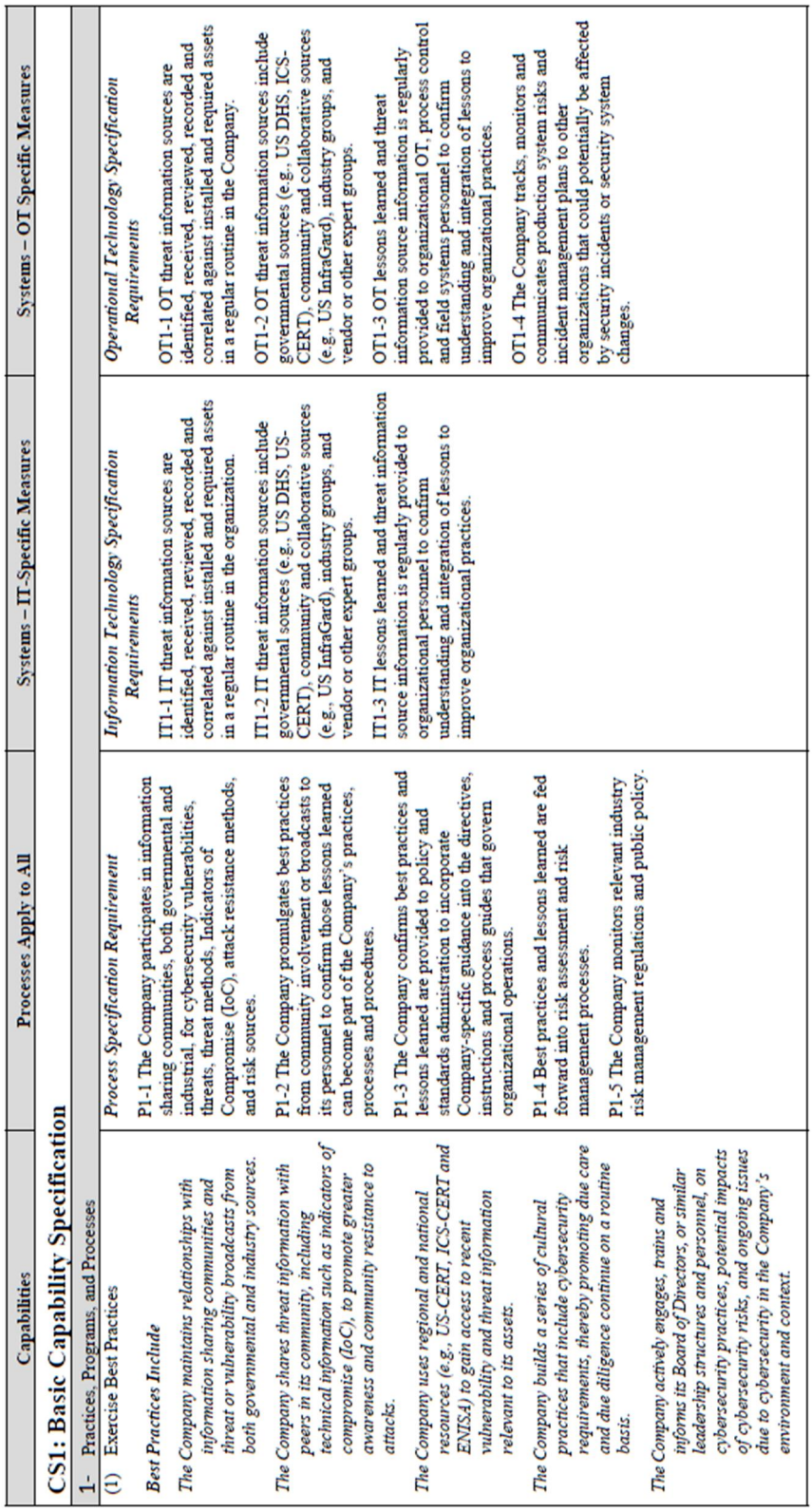


Figure 6: The ABS CyberSafety™ Capability Model (J. Jorgensen 2016, p. 14)

APPENDIX B: THE ABS CYBERSAFETY™ CAPABILITY MATRIX EXAMPLE



Capabilities	Processes Apply to All	Systems – IT-Specific Measures	Systems – OT Specific Measures
CS1: Basic Capability Specification			
1- Practices, Programs, and Processes			
(1) Exercise Best Practices *Best Practices Include* *The Company maintains relationships with information sharing communities and threat or vulnerability broadcasts from both governmental and industry sources.* *The Company shares threat information with peers in its community, including technical information such as indicators of compromise (IoC), to promote greater awareness and community resistance to attacks.* *The Company uses regional and national resources (e.g., US-CERT, ICS-CERT and ENISA) to gain access to recent vulnerability and threat information relevant to its assets.* *The Company builds a series of cultural practices that include cybersecurity requirements, thereby promoting due care and due diligence continue on a routine basis.* *The Company actively engages, trains and informs its Board of Directors, or similar leadership structures and personnel, on cybersecurity practices, potential impacts of cybersecurity risks, and ongoing issues due to cybersecurity in the Company's environment and context.*	*Process Specification Requirement* P1-1 The Company participates in information sharing communities, both governmental and industrial, for cybersecurity vulnerabilities, threats, threat methods, Indicators of Compromise (IoC), attack resistance methods, and risk sources. P1-2 The Company promulgates best practices from community involvement or broadcasts to its personnel to confirm those lessons learned can become part of the Company's practices, processes and procedures. P1-3 The Company confirms best practices and lessons learned are provided to policy and standards administration to incorporate Company-specific guidance into the directives, instructions and process guides that govern organizational operations. P1-4 Best practices and lessons learned are fed forward into risk assessment and risk management processes. P1-5 The Company monitors relevant industry risk management regulations and public policy.	*Information Technology Specification Requirements* IT1-1 IT threat information sources are identified, received, reviewed, recorded and correlated against installed and required assets in a regular routine in the organization. IT1-2 IT threat information sources include governmental sources (e.g., US DHS, US-CERT), community and collaborative sources (e.g., US InfraGard), industry groups, and vendor or other expert groups. IT1-3 IT lessons learned and threat information source information is regularly provided to organizational personnel to confirm understanding and integration of lessons to improve organizational practices.	*Operational Technology Specification Requirements* OT1-1 OT threat information sources are identified, received, reviewed, recorded and correlated against installed and required assets in a regular routine in the Company. OT1-2 OT threat information sources include governmental sources (e.g., US DHS, ICS-CERT), community and collaborative sources (e.g., US InfraGard), industry groups, and vendor or other expert groups. OT1-3 OT lessons learned and threat information source information is regularly provided to organizational OT, process control and field systems personnel to confirm understanding and integration of lessons to improve organizational practices. OT1-4 The Company tracks, monitors and communicates production system risks and incident management plans to other organizations that could potentially be affected by security incidents or security system changes.

Figure 7: Example of the ABS CyberSafety™ Capability Matrix (CyberSafety™ - Volume 2 2016, p. 38)